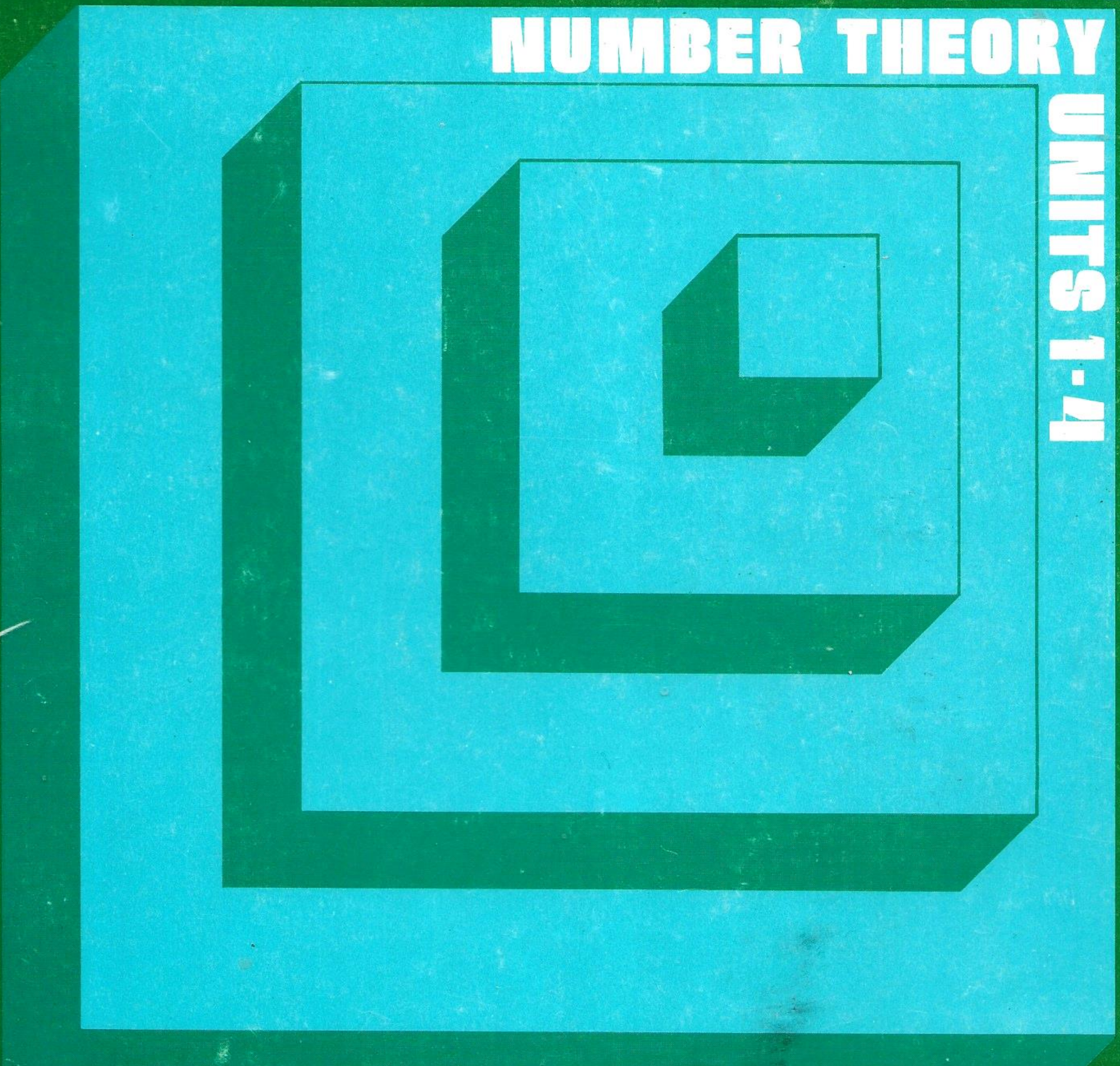
M335 NT 1–4

THE OPEN UNIVERSITY
Mathematics: A Third Level Course
M335 Studies in Pure Mathematics

STUDIES IN PURE MATHEMATICS

NUMBER THEORY

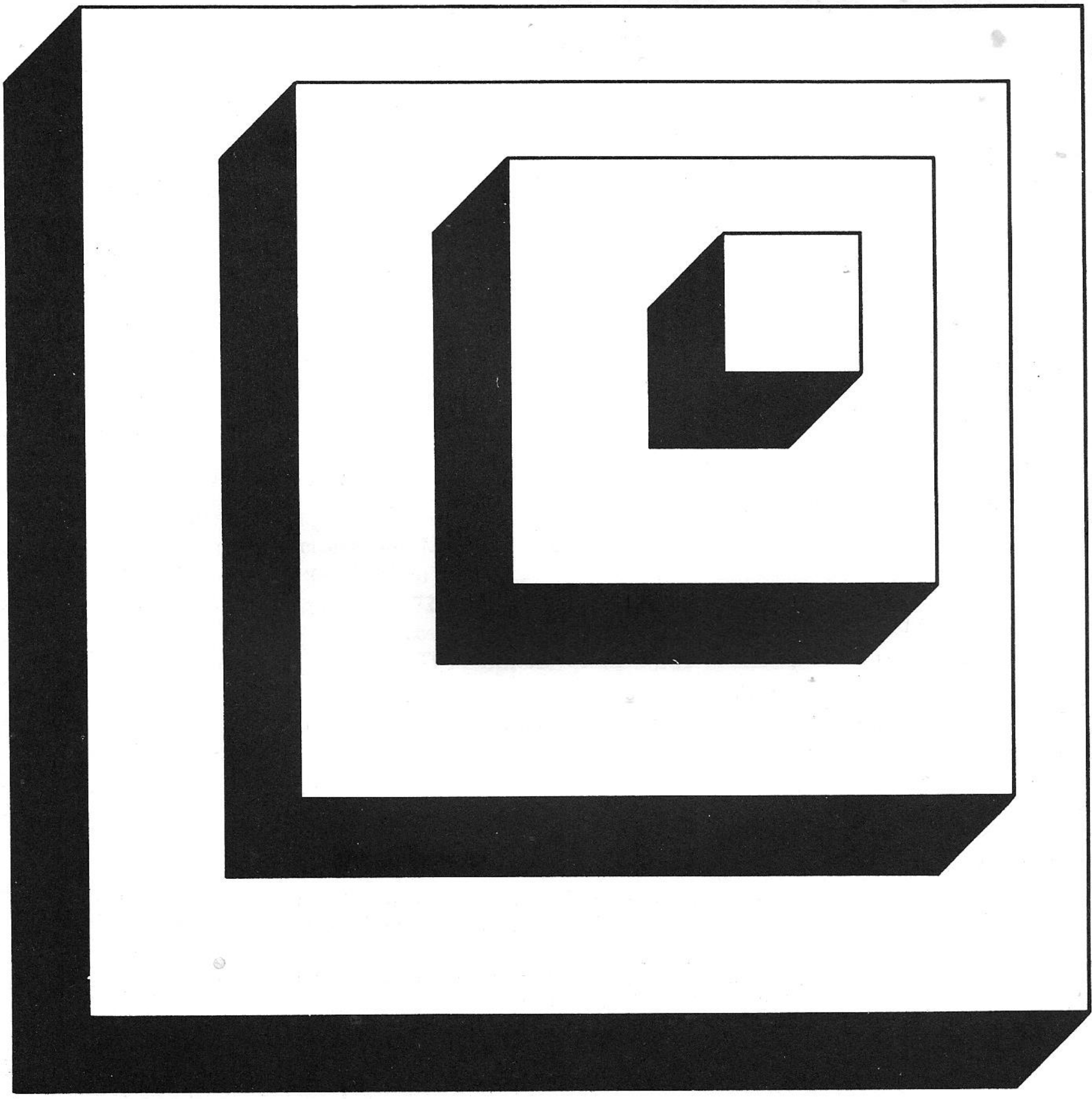
UNITS 1-4



THE OPEN UNIVERSITY
Mathematics: A Third Level Course
M335 Studies in Pure Mathematics
Prepared by the Course Team

NUMBER THEORY

UNITS 1-4



Proviso

Before starting work on this option read the M335 Course Guide. Also, be sure you have a copy of the 1980 (Open University) edition of the set book, *Elementary Number Theory*, by David M. Burton, published by Allyn & Bacon.

The Open University Press, Walton Hall, Milton Keynes.

First published 1982. Reprinted 1984, 1990

Copyright © 1982 The Open University

All rights reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from the publishers.

Produced in Great Britain by
Dotesios Printers Ltd, Trowbridge, Wiltshire.

ISBN 0 335 14010 6

This text forms part of the correspondence element of an Open University Third Level Course.

For general availability of supporting material referred to in this text, please write to Open University Educational Enterprises Limited, 12 Cofferidge Close, Stony Stratford, Milton Keynes MK11 1BY, Great Britain.

Further information on Open University courses may be obtained from: The Admissions Office, The Open University, P.O. Box 48, Milton Keynes MK7 6AB

1.3

Contents

Introduction to the Number Theory option **4**

Unit 1 Basic Ideas

1.0 Introduction **8**
1.1 Mathematical Induction **8**
1.2 The Binomial Theorem **13**
1.3 Early Number Theory **15**
1.4 The Division Algorithm **16**
1.5 The Greatest Common Divisor **19**
1.6 The Euclidean Algorithm **21**
1.7 The Linear Diophantine Equation **23**
1.8 Problem Solving (Tape Section) **25**
1.9 Summary **26**

Unit 2 Primes and their Distribution

2.0 Introduction **28**
2.1 The Fundamental Theorem of Arithmetic **28**
2.2 The Sieve of Eratosthenes **33**
2.3 The Goldbach Conjecture **35**
2.4 The Fibonacci Sequence **37**
2.5 Epilogue **41**
2.6 Summary **42**

Unit 3 Congruence

3.0 Introduction **44**
3.1 Basic Properties of Congruence **44**
3.2 Special Divisibility Tests **50**
3.3 Linear Congruences **52**
3.4 The Fibonacci Sequence Revisited **59**
3.5 Problem Solving (Tape Section) **62**
3.6 Summary **63**

Unit 4 Fermat's Theorem

4.0 Introduction **66**
4.1 Fermat's Factorization Method **66**
4.2 Fermat's Little Theorem **67**
4.3 Wilson's Theorem **72**
4.4 Polynomial Congruences (Tape Section) **75**
4.5 Fermat's and Wilson's Theorems Revisited **81**
4.6 Summary **84**

Introduction

> 'Mathematics is the queen of the sciences and number theory the queen of mathematics.'
>
> Gauss

The Overall Course

This course is one of the options for the Open University half credit course M335: Studies in Pure Mathematics. For information about the overall course, including instructions concerning the continuous assessment and final examination, see Guide to the Course M335.

The Set Textbook

The set textbook for the course is the 1980 Open University Edition of *Elementary Number Theory* by David M. Burton, published by Allyn and Bacon. It is essential that you possess a copy of this edition.

It is inconceivable that for a course of this length we could complete the whole of Burton's book, and consequently some parts have had to be missed out. To get the right foundations we must start at the very beginning of the book, but we also felt that we should like to reach the later chapters, which cover some of the more famous and interesting topics in the subject. To achieve this we have pursued a careful path through the text, omitting several sections from the middle parts of the book.

Of course, there is no reason why you should not read for yourself the sections that we have chosen to omit. We emphasize that nothing has been left out because it is in any way unsuitable (or uninteresting!), but merely because of the need to present an acceptable total amount of material for assessment purposes.

The Course Units

The overall material has been divided into eight more or less equal parts which we present as 'units'. Each unit, including the associated assessment materials, is intended to involve you in about 10–12 hours work.

Our unit texts consist of guided tours through the relevant parts of the set textbook, which we refer to as **B** (for Burton). They comprise commentary and notes on the text of **B**, supplementary text, worked examples (the ends of which are marked □, if necessary) and self-assessment questions (SAQs) with solutions (the ends of which are marked ■). Additional exercises for each unit appear in the Exercise Booklet, bound separately from the main unit text.

Each unit is subdivided into sections which, as a rule, correspond to sections of **B**. There are however several instances where we have broken long sections of **B** into parts. Most units have four or five sections corresponding very roughly to an 'evening's work' each. *Unit 1* is an exception, having eight shorter sections. Examples and SAQs are numbered in order, starting at 1 in each unit.

The referencing in our texts will always clarify whether we are referring to **B** or to one of our units. The reading passages are clearly indicated; for instance

READ B from page 54, line 11 to the end of Section 3.2.

Most reading passages are accompanied by some notes in the unit text, the notes being referenced by a line in **B**. (Line $-n$ denotes the nth line up from the bottom of the page; the end of the note is marked ▲.)

The Role of Problems

Whilst number theory is arguably the purest of all subjects within mathematics, you must not form the impression that it is all about development of theories and proofs of theorems. On the contrary, number theory is about problem solving. Nobody masters the calculus by just reading about it; it is essential to practise differentiation and integration on a large number of examples. The same is true of number theory. You cannot get to grips with number theory without solving problems yourself.

To this end we have included a good stock of self-assessment questions in all units and you should always have pencil and paper at hand. The Examples in the units are for you to read, but the SAQs are for you to *do*. Do not spend forever on a problem which looks like defeating you. If you get stuck you should refer to the solution that is there—but do not give in too easily!

Further problems (and their solutions) on each unit can be found in the Exercise Booklet. It is not intended that you should work through all of these. If you feel confident that you have mastered a certain section then there will be no need to attempt further problems on that section. On the other hand, where a section has proved to be heavy going the additional problems will be most valuable.

The Exercise Booklet also contains a number of *challenge problems*. These are intended only for the 'high fliers' who enjoy a hard challenge, being pitched at a level above the expected attainment from the course.

Course Structure

The course has a linear structure. By this we mean that the units should be studied in order, for each is in some way dependent on its predecessors. The exception to this rule is *Unit 7* (on which the first section of *Unit 8* depends). This stands alone and can be studied at any time after *Unit 3*.

Tape Sections

Four of the units contain tape sections. For these you will need access to a cassette player. In working these sections you will, as always, need pencil and paper handy, and a pause or stop button within easy reach.

Calculator

The nature of number theory has changed dramatically over the past few years, due to the advent of the computer. Computations which were well nigh impossible only a few years ago can now be managed with ease, with the result that substantial numerical evidence supporting (or toppling) outstanding conjectures is being gathered all the time. Although the material in this course presents many challenges for those with access to a computer, we have written the course to avoid the computational side of the subject, thereby making it accessible to all. There are, however, many problems in the course which will be simplified if you possess a *calculator* and, although this is not essential, it is advisable that you have one. The calculator recommended for your Foundation Course will be more than adequate.

Course Team

The course has been written by Alan Best and Bob Coates, with contributions from David Asche, Andrew Brown, Francis Coghlan, Stanley Collings, David Crowe (Editor) and Hossein Zand.

Dedication

To the memory of Don Mansfield.

UNIT 1
BASIC IDEAS

1.0 Introduction

This first unit comprises Chapters 1 and 2 of **B** (the set book by Burton). The objective of the unit is to lay a firm foundation for the whole course by examining in detail the fundamental ideas which form the basis from which to study properties of numbers.

Chapter 1 reviews two topics: *proof by mathematical induction* and the *Binomial Theorem*. You will probably already be familiar with both these ideas (although you might find the approach to mathematical induction in **B** somewhat different from, for example, that in our Foundation Course). The chapter ends with a section on the early history of number theory. Throughout **B** we shall encounter these short, interesting historical extracts which, although not forming an assessable part of the course, we encourage you to read.

From an early age we all learn how to divide one integer by another obtaining a quotient and a remainder. The result we use here is known as the *Division Algorithm* and is expounded at the beginning of Chapter 2. As you will quickly appreciate, the consequences of this simple idea, both practical and theoretical, make it a cornerstone of number theory. The later sections of the chapter develop these consequences and, in particular, introduce the *greatest common divisor*—a topic which again ought to be familiar and one which is going to figure prominently throughout the course.

If you have a prior knowledge of prime numbers, there might well be a temptation to use them in connection with divisibility problems. But notice that prime numbers are not introduced in **B** until Chapter 3, and we do not involve them in this unit. The development of the material in **B** is logically sound. For instance, Euclid's Lemma (Theorem 2-5, **B** page 28) must seem entirely obvious and capable of 'proof' in a couple of lines to anyone who knows anything at all about prime numbers. But in the next chapter, Euclid's Lemma is used extensively to establish properties of prime numbers; so to use properties of primes to prove Euclid's Lemma would plainly lead to circular arguments.

In this course we shall develop a lot of theory and investigate many of the classical results in the subject. However, the course will contain a heavy emphasis on 'problem solving', and you will find a plentiful supply of worked examples and SAQs (with solutions) in all units. This unit ends with a section on problem solving. The text presents a number of problems which are related to ideas in the unit but which are slightly more difficult then previous SAQs. Guidance on how to go about solving them is on the accompanying tape cassette. The solutions themselves appear in the Exercise Booklet.

1.1 Mathematical Induction

Every teacher and every textbook writer must assume that his students or readers come with a minimal amount of prior knowledge of the subject. **B** assumes that you are familiar with certain elementary facts about the integers—positive, negative and zero.

Firstly he assumes that you know the usual rules for addition and multiplication, including the cancellation law, i.e.

$$\text{if } ab = ac \text{ where } a, b \text{ and } c \text{ are integers and } a \neq 0, \text{ then } b = c.$$

Secondly he assumes that you know the rules for inequalities. For example, if $a \geq b$ and $c < 0$ (i.e. c is negative) then $ac \leq bc$.

Lastly he assumes that you have seen the 'Well-ordering Principle' which states that if S is a non-empty set of non-negative integers then S has a least element. In fact this principle may be new to you but, as you will see, it turns out to be very powerful and enables us to deduce as a *theorem* the Principle of Mathematical Induction in all its various forms.

READ B Section 1.1, page 2, as far as page 6, line 15.

NOTES (i) *Page 2, last line*
In specifying a set, in this case S, **B** uses the symbol '|' to stand for 'such that'. From other Open University courses you are probably more familiar with the use of ':' for this purpose.

(ii) *Page 3, line 14*
This statement of the Principle of Finite Induction might strike you as unfamiliar because of the presence of the set S. If so, **B**'s 'remark' on page 5 should explain how the statement relates to the usual way we write out proofs using Mathematical Induction. We merely show that

(i) the result is true for the integer 1 (the basis for the induction), and that

(ii) if the result is true for any positive integer k then it is true for $k + 1$ (the induction step).

The unmentioned set S is the set of all positive integers for which the result is true. So proving that S is the set of all positive integers is the same as showing that the result is true for all positive integers. ▲

SAQ 1 **B** page 8, Problems 1.1, number 1, parts (a) and (e).

SAQ 2 **B** page 9, Problems 1.1, number 2.

SOLUTION TO SAQ 1 (Like **B** we shall suppress mention of the set S.)

(a) The result is true when $n = 1$ since

$$1 = \frac{1 \cdot 2}{2} \qquad \text{(basis for induction).}$$

Assume true for $n = k$, i.e.

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2} \qquad \text{(induction hypothesis).}$$

Then adding $k + 1$ to both sides gives

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)(k+2)}{2} \qquad \text{(induction step)} \end{aligned}$$

showing the result to be true when $n = k + 1$. Therefore by the First Principle of Finite Induction the result is true for all integers $n \geq 1$.

(e) The result is true for $n = 1$ since

$$1^3 = \left(\frac{1 \cdot 2}{2}\right)^2 \qquad \text{(basis for induction).}$$

Assume true for $n = k$, i.e.

$$1^3 + 2^3 + \cdots + k^3 = \left(\frac{k(k+1)}{2}\right)^2 \qquad \text{(induction hypothesis).}$$

Then adding $(k+1)^3$ to both sides gives

$$\begin{aligned}1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3\\ &= \frac{(k+1)^2(k^2+4k+4)}{4}\\ &= \left(\frac{(k+1)(k+2)}{2}\right)^2 \qquad \text{(induction step)}\end{aligned}$$

showing the result to be true for $n = k + 1$.

Therefore, by the First Principle of Finite Induction, the result is true for all integers $n \geq 1$. ■

SOLUTION TO SAQ 2 The result is true for $n = 1$ since

$$\frac{a(r^{1+1}-1)}{r-1} = \frac{a(r-1)(r+1)}{r-1} = a + ar \qquad \text{(basis for induction).}$$

Assume that

$$a + ar + ar^2 + \cdots + ar^k = \frac{a(r^{k+1}-1)}{r-1} \qquad \text{(induction hypothesis).}$$

Adding ar^{k+1} to both sides gives

$$\begin{aligned}a + ar + ar^2 + \cdots + ar^k + ar^{k+1} &= \frac{a(r^{k+1}-1)}{r-1} + ar^{k+1}\\ &= \frac{a(r^{k+1}-1) + ar^{k+1}(r-1)}{r-1}\\ &= \frac{a(r^{k+2}-1)}{r-1} \qquad \text{(induction step)}\end{aligned}$$

showing the result is true for $n = k + 1$.

Therefore, by the First Principle of Finite Induction, the result is true for all integers $n \geq 1$.

COMMENT There is in fact an easier way of obtaining this result, without using mathematical induction. If we let

$$S = a + ar + ar^2 + \cdots + ar^n$$

then

$$rS = \qquad ar + ar^2 + \cdots + ar^n + ar^{n+1}$$

and subtraction gives

$$S - rS = a - ar^{n+1}$$

which produces the required result. ■

READ B page 6, line 16 to line -4.

The following example will illustrate a situation where the Second Principle of Finite Induction becomes a necessity because of the nature of the problem.

EXAMPLE 1 Suppose we are given a sequence $\{a_i\}$ of non-negative integers defined by the condition

$$a_0 = 1 \quad \text{and} \quad a_n = \sum_{i=0}^{n-1} a_i, \text{ for } n \geq 1.$$

(This complicated looking definition of the terms merely says that each is the sum of all the previous ones.) We shall prove, using the Second Principle of

Mathematical Induction, that

$$a_n = 2^{n-1}, \qquad \text{for all integers } n \geq 1.$$

Firstly the result is true when $n = 1$ since $a_1 = 1$ and $2^{1-1} = 1$. Now suppose the result is true for all the positive integers less than or equal to k, i.e. $a_i = 2^{i-1}$ for all integers i such that $1 \leq i \leq k$. (This is the induction hypothesis and, as usual, we are suppressing all reference to the set S of positive integers for which the result is true.)

By definition,

$$a_{k+1} = \sum_{i=0}^{k} a_i = a_0 + \sum_{i=1}^{k} a_i.$$

Now we use the induction hypothesis, and this is where you should see that it is the Second Principle that we really need.

$$\begin{aligned} a_{k+1} &= 1 + \sum_{i=1}^{k} 2^{i-1} \\ &= 1 + \frac{2^k - 1}{2 - 1} \qquad \text{(by SAQ 2 with } a = 1, r = 2 \text{ and } n = k - 1) \\ &= 2^k. \end{aligned}$$

So the result is true when $n = k + 1$. This completes the induction step and so, by the Second Principle of Finite Induction, $a_n = 2^{n-1}$ for all integers $n \geq 1$.

SAQ 3 A sequence $\{a_i\}$, $i \geq 1$ is defined by

$$a_1 = 3 \quad \text{and} \quad a_n = \left(\sum_{i=1}^{n-1} a_i\right) + 3, \quad \text{for all integers } n \geq 2.$$

Show that $a_n = 3 \cdot 2^{n-1}$ for all integers $n \geq 1$.

$a_1 = 3 = 3 \cdot 2^{1-1}$ so the result is true when $n = 1$.

SOLUTION TO SAQ 3 Assume the result is true for all the positive integers less than or equal to k, i.e. $a_i = 3 \cdot 2^{i-1}$ for all integers i such that $1 \leq i \leq k$. Then, by definition,

$$\begin{aligned} a_{k+1} &= \left(\sum_{i=1}^{k} a_i\right) + 3 \\ &= \left(\sum_{i=1}^{k} 3 \cdot 2^{i-1}\right) + 3 \\ &= 3 \cdot \frac{2^k - 1}{2 - 1} + 3 \qquad \text{(by SAQ 2 with } a = 3, r = 2 \text{ and } n = k - 1) \\ &= 3 \cdot 2^k. \end{aligned}$$

So the result is true when $n = k + 1$, and therefore, by the Second Principle of Finite Induction, the result is true for all integers $n \geq 1$. ■

READ B page 6, line −3 to the end of Section 1.1.

NOTES (i) *Page 7, line 6*

In the generalized form referred to, the statements of the First Principle become

(a) n_0 belongs to S, and

(b) whenever the integer $k \geq n_0$ is in S, then the next integer $k + 1$ must also be in S.

The conclusion is as given.

(ii) You may have noticed that **B** sometimes takes the induction step from k to $k+1$, as in the original statement of the Principle, and sometimes from $k-1$ to k. In the next section he will go from m to $m+1$. All are equally valid since all that matters is that the induction step takes us from one general integer to its successor. ▲

EXAMPLE 2 As a final example in this section we shall prove that $2^n > n^3$ for all integers $n \geq 10$. The induction step here is not as direct as in previous examples.

The result is true when $n = 10$ since

$$2^{10} = 1024 > 1000 = 10^3.$$

We next assume that $2^k > k^3$ where $k \geq 10$ is some integer and our objective is to prove that $2^{k+1} > (k+1)^3$. Now

$$2^{k+1} = 2 \cdot 2^k > 2k^3$$

so if we can show that $2k^3 > (k+1)^3$ we are finished. But

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1$$

and (i) $1 < k^3/3$, since $k \geq 10$;

(ii) as $3 < k$, $9 < k^2$ and so, multiplying by $\frac{k}{3}$, $3k < k^3/3$;

(iii) as $10 \leq k$, $3 < k/3$ and so $3k^2 < k^3/3$.

Combining these facts,

$$(k+1)^3 < k^3 + k^3/3 + k^3/3 + k^3/3 = 2k^3$$

as required. ☐

The induction step in Example 2 could have been tackled in many other ways. Here is an alternative approach which illustrates the point that although the result to be proved is true for all integers $k \geq 10$, the induction step holds for all integers $k \geq 4$.

To show $2k^3 > (k+1)^3$ for $k \geq 4$.

Rearranging the inequality we are required to show that

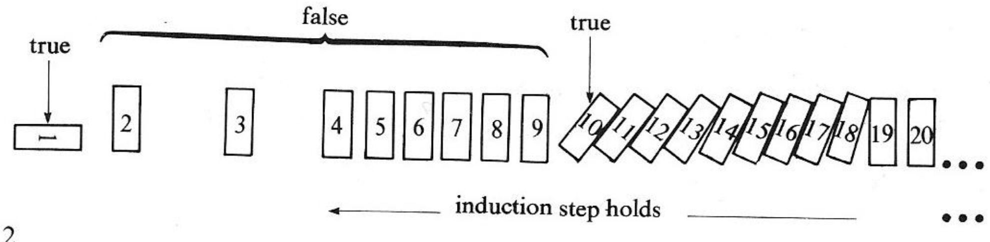
$$\frac{(k+1)^3}{k^3} < 2, \text{ or } \left(1 + \frac{1}{k}\right)^3 < 2, \text{ for } k \geq 4.$$

Now as k increases, $\frac{1}{k}$ decreases, and so the greatest value of $1 + 1/k$ is given by the least value of k, namely $k = 4$. So

$$\left(1 + \frac{1}{k}\right)^3 \leq \left(1 + \frac{1}{4}\right)^3 \simeq 1.953 < 2, \text{ for } k \geq 4$$

as required.

We have the curious situation where the result $2^n > n^3$ is true for $n \geq 10$, and also true for $n = 1$, $(2^1 > 1^3)$, but false for $n = 2, 3, \ldots, 9$. (Try them and see!) Yet we have proved that the induction step works for all integers from $n = 4$ onwards. But notice that from these facts we cannot deduce that $2^n > n^3$ for all $n \geq 1$ (since the induction step fails for $n = 1$), nor can we deduce that $2^n > n^3$ for all $n \geq 4$ (since, despite the fact that the induction step holds, the result is false for $n = 4$). Drawing on **B**'s anology with the dominoes, the situation is depicted by



If any domino after the third is knocked over, all subsequent ones fall. The first two knocked over are numbers 1 and 10.

SAQ 4 **B** page 9, Problems 1.1, number 7.

SOLUTION TO SAQ 4 The result is true when $n = 1$ since $1(1!) = 2! - 1$.

Assume the result is true when $n = k$, i.e.

$$1(1!) + 2(2!) + \cdots + k(k!) = (k+1)! - 1.$$

Adding $(k + 1)\,((k + 1)!)$ to both sides gives

$$\begin{aligned}1(1!) + 2(2!) + \cdots + (k+1)\,((k+1)!) &= (k+1)! - 1 + (k+1)\,((k+1)!)\\ &= (k+2)\,(k+1)! - 1\\ &= (k+2)! - 1\end{aligned}$$

showing the result to be true when $n = k + 1$. By the First Principle of Finite Induction, the result is true for all integers $n \geq 1$. ■

1.2 The Binomial Theorem

This section discusses the Binomial Theorem, which you met in the Foundation Course. There we used the notation ${}^{n}C_{r}$ for the binomial coefficients; **B** uses the alternative notation $\binom{n}{r}$.

READ B Section 1.2, pages 9–12.

NOTES (i) *Page 10, line 9*

One way of remembering Pascal's Rule is to think of the binomial coefficient $\binom{n}{k}$ as being the number of ways of choosing k objects from n. There are $\binom{n+1}{k}$ ways of choosing k objects from $n + 1$ objects. Either we choose the first one or we do not. If we do not then we are left to choose the k from the remaining n, which we can do in $\binom{n}{k}$ ways. On the other hand, if we do choose the first object we need only choose $k - 1$ from the remaining n, giving the coefficient $\binom{n}{k-1}$.

(ii) *Page 12 lines 6–11*

If you have difficulty sorting out **B**'s proof of the Binomial Theorem, keep your eye on the term involving b^k in the expansion of $(a + b)^{m+1}$. If k is neither 0 nor $m + 1$ then, by the equation in line 4, this term is the sum of

(a) a times the term in b^k in the expansion of $(a + b)^m$

and

(b) b times the term in b^{k-1} in the expansion of $(a + b)^m$.

That is, using the induction hypothesis,

$$\begin{aligned}a\binom{m}{k} a^{m-k} b^k + b\binom{m}{k-1} a^{m-k+1} b^{k-1} &= \left[\binom{m}{k} + \binom{m}{k-1}\right] a^{m-k+1} b^k\\ &= \binom{m+1}{k} a^{m+1-k} b^k,\end{aligned}$$

by Pascal's Rule.

Now $k = 0$ and $k = m + 1$ have to be handled separately. If $k = 0$ then $b(a + b)^m$ contributes nothing to the term involving b^0 while if $k = m + 1$ then $a(a + b)^m$ contributes nothing to the term involving b^{m+1}, and this is why **B** isolates the terms a^{m+1} and b^{m+1}. This is the essence of **B**'s argument, but he uses summation notation and handles all values of k at the same time. ▲

SAQ 5 **B** page 12, Problems 1.2, number 1.

SAQ 6 **B** page 12, Problems 1.2, number 4.

SOLUTION TO SAQ 5 (a) We first observe that $k \geq 0$ for the binomial coefficients to be defined. Now

$$\begin{aligned}\binom{n}{k} < \binom{n}{k+1} &\Leftrightarrow \frac{n!}{k!\,(n-k)!} < \frac{n!}{(k+1)!\,(n-k-1)!}\\ &\Leftrightarrow \frac{(k+1)!}{k!} < \frac{(n-k)!}{(n-k-1)!}\\ &\Leftrightarrow k + 1 < n - k\\ &\Leftrightarrow k < \tfrac{1}{2}(n-1), \text{ as required.}\end{aligned}$$

(b) Replacing $<$ by $=$ in (a) we see that

$$\binom{n}{k} = \binom{n}{k+1} \Leftrightarrow k = \tfrac{1}{2}(n-1)$$

and as k is an integer this implies that $n - 1$ is even, i.e. n is odd. ■

SOLUTION TO SAQ 6 (a) The result is true when $n = 2$ since $\binom{2}{2} = 1 = \binom{3}{3}$.

Assume that $\binom{2}{2} + \binom{3}{2} + \cdots + \binom{k}{2} = \binom{k+1}{3}$.

Then, adding $\binom{k+1}{2}$ to both sides gives

$$\begin{aligned}\binom{2}{2} + \binom{3}{2} + \cdots + \binom{k}{2} + \binom{k+1}{2} &= \binom{k+1}{3} + \binom{k+1}{2}\\ &= \binom{k+2}{3}, \qquad \text{by Pascal's Rule.}\end{aligned}$$

By the First Principle of Finite Induction, the result is true for all integers $n \geq 2$.

(b) Adding together the equations $2\binom{m}{2} + m = m^2$, for $m = 2, 3, \ldots, n$, we obtain

$$\sum_{m=2}^{n} 2\binom{m}{2} + \sum_{m=2}^{n} m = \sum_{m=2}^{n} m^2.$$

Therefore $2\binom{n+1}{3} + \dfrac{n(n+1)}{2} - 1 = \displaystyle\sum_{m=1}^{n} m^2 - 1$ (as in the result of SAQ 1(a)).

That is,

$$\begin{aligned}\sum_{m=1}^{n} m^2 &= \frac{2(n+1)\,n(n-1)}{3\cdot 2\cdot 1} + \frac{n(n+1)}{2}\\ &= \frac{2(n+1)\,n(n-1) + 3n(n+1)}{6}\\ &= \frac{1}{6}n(n+1)\,(2n+1).\end{aligned}$$

COMMENT You might like to think of the result of SAQ 6(a) in the following way. $\binom{n+1}{3}$ is the number of ways of choosing 3 objects from $n + 1$ objects. Now either you choose the first object or you do not. If you do choose the first object then you choose the 2 further objects from the remaining n objects, giving the binomial coefficient $\binom{n}{2}$. On the other hand, if you do not choose the first object then consider whether or not you choose the second object. If you do choose the second object then you choose the 2 further objects from the $n - 1$ remaining, giving the binomial coefficient $\binom{n-1}{2}$, and so on. ■

1.3 Early Number Theory

Throughout the book, **B** includes numerous short historical sections such as the next reading passage. The historical perspective given by these sections should give you a greater appreciation of the subject itself.

READ B Section 1.3, pages 13–16.

SAQ 7 **B** page 16, Problems 1.3, number 1.

SOLUTION TO SAQ 7

(a) This is precisely the solution of SAQ 1(a), i.e.

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

(b) Let n be a triangular number, so that $n = \dfrac{r(r+1)}{2}$ for some integer $r \geq 1$. Then

$$8n + 1 = 4r(r+1) + 1 = (2r+1)^2,$$

a perfect square.

On the other hand, if $8n + 1$ is a perfect square we can write $8n + 1 = k^2$, for some positive integer k. But $8n + 1$ is odd and so k must be odd (the square of any even integer being even). So $k = 2r + 1$ for some integer $r \geq 1$ and $8n + 1 = (2r+1)^2 = 4r(r+1) + 1$, giving $n = \dfrac{r(r+1)}{2}$, a triangular number.

(c) Consecutive triangular numbers are $\dfrac{r(r+1)}{2}$ and $\dfrac{(r+1)(r+2)}{2}$ whose sum is $(r+1)^2$, a perfect square.

(d) Let $n = \dfrac{r(r+1)}{2}$, for some integer $r \geqslant 1$. Then

$$\begin{aligned} 9n + 1 &= 9\frac{r(r+1)}{2} + 1 = \frac{9r^2 + 9r + 2}{2} \\ &= \frac{(3r+1)(3r+2)}{2} \\ &= \frac{k(k+1)}{2}, \qquad \text{where } k = 3r + 1. \end{aligned}$$

Similarly,

$$25n + 3 = \frac{(5r + 2)(5r + 3)}{2}$$

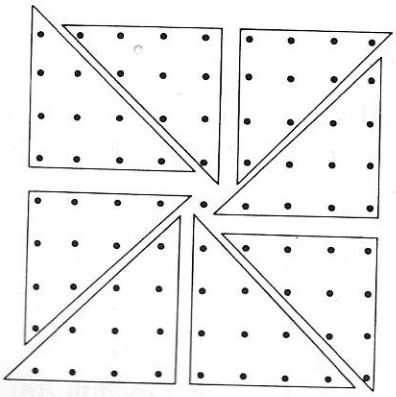
and

$$49n + 6 = \frac{(7r + 3)(7r + 4)}{2}$$

both of which are triangular numbers.

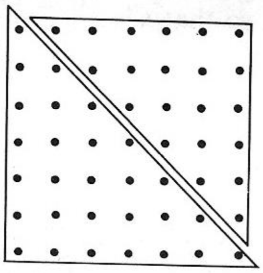
COMMENT The results of parts (b) and (c) can be illustrated as follows.

(b)



Here we have taken $n = 10$ (i.e. $r = 4$), and shown how the 8 triangles of dots, plus the dot in the middle, form a square with 9 (i.e. $2r + 1$) dots along each side.

(c)



Here we have taken $r = 6$ and shown how the two triangles give a square having 7 (i.e. $r + 1$) dots along each side. ■

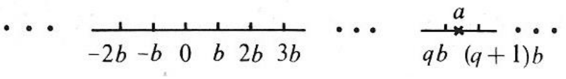
1.4 The Division Algorithm

This section is devoted to the Division Algorithm. This result tells us that we can divide one integer by another to obtain a quotient and a remainder; for example, we can divide 23 by 4 to obtain a quotient of 5 and a remainder of 3 or rather more formally $23 = 5 \cdot 4 + 3$. But more than this, it tells us that the quotient and remainder are unique; for the example given above this means that if $23 = q \cdot 4 + r$ where $0 \leq r < 4$, then $q = 5$ and $r = 3$. This familiar result, which you probably learned at a very early age, is of enormous theoretical importance and in the remaining sections of the unit we shall develop certain consequences of it which are fundamental to our treatment of the theory of numbers.

READ B Section 2.1, pages 20–22.

NOTE *Page 20, line 14*

As the result itself is so familiar, it may come as something of a shock to discover how complicated the proof seems. You can get an intuitive grasp of the Division Algorithm by imagining all the multiples of the positive integer b stepped off along the real line.



Whatever the value of the integer a it will lie between two adjacent marks. More precisely,

$$qb \le a < (q+1)b$$

or

$$0 \le a - qb < b.$$

Once we put $r = a - qb$, i.e. $a = qb + r$, this gives the desired result. In the proof the existence of such a (unique) q is verified by choosing the one which gives the smallest non-negative value for $a - qb$. ▲

EXAMPLE 3 We shall show as an example that every sixth power of an integer is of the form $7k$ or of the form $7k + 1$.

By the Division Algorithm, any integer can be expressed in the form $7k + r$ where $r = 0, 1, 2, 3, 4, 5$ or 6, so we proceed to investigate the sixth powers of such numbers. By the Binomial Theorem,

$$(7k + r)^6 = 7 \cdot (\text{polynomial in } k) + r^6$$

(since in the expansion of $(a + b)^6$ every term contains a positive power of a, with the exception of the final term b^6, and we are putting $a = 7k$ and $b = r$).

Therefore

$$\begin{aligned}
(7k+0)^6 &= 7 \cdot P_0(k) + 0^6 & &= 7 \cdot P_0(k),\\
(7k+1)^6 &= 7 \cdot P_1(k) + 1^6 & &= 7 \cdot P_1(k) + 1,\\
(7k+2)^6 &= 7 \cdot P_2(k) + 2^6 = 7 \cdot P_2(k) + 64 & &= 7 \cdot (P_2(k) + 9) + 1,\\
(7k+3)^6 &= 7 \cdot P_3(k) + 3^6 = 7 \cdot P_3(k) + 729 & &= 7 \cdot (P_3(k) + 104) + 1,\\
(7k+4)^6 &= 7 \cdot P_4(k) + 4^6 = 7 \cdot P_4(k) + 4096 & &= 7 \cdot (P_4(k) + 585) + 1,\\
(7k+5)^6 &= 7 \cdot P_5(k) + 5^6 = 7 \cdot P_5(k) + 15625 & &= 7 \cdot (P_5(k) + 2232) + 1,\\
(7k+6)^6 &= 7 \cdot P_6(k) + 6^6 = 7 \cdot P_6(k) + 46656 & &= 7 \cdot (P_6(k) + 6665) + 1.
\end{aligned}$$

Thus all the sixth powers are of the form $7k$ or $7k + 1$.

The calculations above were worthwhile, if only to illustrate how much labour is saved by some of the theorems we prove later. However, there is one simplification which is worth a mention. Any number of the form $7k + 6$ is also of the form $7k - 1$ (for a different value of k, of course) and

$$\begin{aligned}
(7k-1)^6 &= 7 \cdot (\text{polynomial in } k) + (-1)^6\\
&= 7 \cdot (\text{polynomial in } k) + 1
\end{aligned}$$

and so we have avoided taking the sixth power of 6. Similar economies are obtained by noting that any number of the form $7k + 5$ is also of the form $7k - 2$ and so on.

SAQ 8 **B** page 22, Problems 2.1, number 3.

SAQ 9 Prove that every fourth power of an integer is of the form $5k$ or $5k + 1$.

SAQ 10 **B** page 23, Problems 2.1, number 6. (This is the version of the Division Algorithm which enabled us to make the simplification in Example 3 and in our Solution to SAQ 9.)

SOLUTION TO SAQ 8

(a) The Division Algorithm tells us that any integer is representable in one of the four forms $4k$, $4k + 1$, $4k + 2$ or $4k + 3$ (the integer is a multiple of 4 with a remainder 0, 1, 2 or 3). Of these, $4k = 2(2k)$ and $4k + 2 = 2(2k + 1)$ are both even, whilst $4k + 1 = 2(2k) + 1$ and $4k + 3 = 2(2k + 1) + 1$ are both odd, i.e. are of the form $2n + 1$.

(b) Any integer is of one of the three forms $3k$, $3k + 1$ or $3k + 2$. Squaring, we obtain

$$\begin{aligned}(3k)^2 &= 3(3k^2)\\(3k+1)^2 &= 3(3k^2+2k)+1\\(3k+2)^2 &= 3(3k^2+4k+1)+1\end{aligned}$$

so that any square is of the form $3n$ or $3n + 1$.

(c) Using the same technique as in (b),

$$\begin{aligned}(3k)^3 &= 9(3k^3)\\(3k+1)^3 &= 9(3k^3+3k^2+k)+1\\(3k+2)^3 &= 9(3k^3+6k^2+4k)+8\end{aligned}$$

which are of the required forms. ■

SOLUTION TO SAQ 9

Any integer is of the form $5k$, $5k + 1$, $5k + 2$, $5k + 3$ or $5k + 4$. As in Example 3, we can simplify the solution by taking the alternative forms $5k - 2$ for $5k + 3$ and $5k - 1$ for $5k + 4$.

$$\begin{aligned}(5k)^4 & &&= 5\cdot P_0(k)\\(5k+1)^4 &= 5\cdot P_1(k)+1^4 &&= 5\cdot P_1(k)+1\\(5k+2)^4 &= 5\cdot P_2(k)+2^4 &&= 5\cdot(P_2(k)+3)+1\\(5k-2)^4 &= 5\cdot P_3(k)+(-2)^4 &&= 5\cdot(P_3(k)+3)+1\\(5k-1)^4 &= 5\cdot P_4(k)+(-1)^4 &&= 5\cdot P_4(k)+1\end{aligned}$$

so the fourth power of any integer is of the form $5k$ or of the form $5k + 1$. ■

SOLUTION TO SAQ 10

Following the hint in **B**, by the Division Algorithm there are unique q' and r' with $0 \le r' < |b|$ where $a = q'b + r'$. If $0 \le r' \le \frac{1}{2}|b|$, we let $r = r'$ and $q = q'$ so $a = qb + r$ and $0 \le r \le \frac{1}{2}|b|$. If, on the other hand, $\frac{1}{2}|b| < r' < |b|$, let $r = r' - |b|$ so $-\frac{1}{2}|b| < r < 0$. This gives $a = q'b + r + |b|$. Now if $b > 0$ then $|b| = b$ and we get $a = (q' + 1)\,b + r$ but if $b < 0$ then $|b| = -b$ and we get $a = (q' - 1)\,b + r$. This is why **B** suggests we take $q = q' + 1$ if $b > 0$ and $q = q' - 1$ if $b < 0$, so that whatever the sign of b we obtain $a = qb + r$.

Now combining the situations we get $a = qb + r$ where $-\frac{1}{2}|b| < r \le \frac{1}{2}|b|$. It remains to prove that q and r are unique, so suppose that in addition $a = q_1b + r_1$, where $-\frac{1}{2}|b| < r_1 \le \frac{1}{2}|b|$. Following the proof of the Division Algorithm, the equations $a = qb + r$ and $a = q_1b + r_1$ give

$$|q - q_1|\,|b| = |r_1 - r|. \qquad (*)$$

Now adding the inequalities $-\frac{1}{2}|b| \le -r < \frac{1}{2}|b|$ and $-\frac{1}{2}|b| < r_1 \le \frac{1}{2}|b|$ gives $-|b| < r_1 - r < |b|$ or equivalently $|r_1 - r| < |b|$. Substituting this in $(*)$ we get $|q - q_1|\,|b| < |b|$ which leads to $|q - q_1| < 1$ and as $|q - q_1|$ is a non-negative integer this implies that $q = q_1$ which in turn leads to $r = r_1$, completing the proof of the uniqueness of q and r. ■

1.5 The Greatest Common Divisor

The greatest common divisor (or highest common factor) of two integers usually assumes a transient importance in school work; it then vanishes rarely to be met again. In the theory of numbers it is of vital significance. The results of this subsection are of crucial importance in this course, so make sure now that you understand them, and how to use them.

The first reading passage is concerned with basic divisibility properties of integers.

READ B from the beginning of Section 2.2 on page 23 as far as page 24, line -8.

NOTE The proofs of parts (1) to (5) of Theorem 2-2 are straightforward. By all means take up **B**'s invitation to try them as an exercise, but here are the missing proofs:

(1) For all a, $0 = a \cdot 0$ so $a|0$ (by Definition 2-1)
and $a = 1 \cdot a$ so $1|a$
and $a = a \cdot 1$ so $a|a$.

(2) $a|1$ if there is an integer c such that $ac = 1$. (From our knowledge of the integers it is apparent that $a = c = \pm 1$. But for completeness we shall prove that fact using properties of inequalities.) Now if a is positive then so is c since their product is 1 (which is positive); therefore as 1 is the least positive integer we know that $c \geq 1$. We can now multiply this inequality by the positive integer a and obtain $ac \geq a$, i.e. $1 \geq a$, which means $a = 1$ since we assumed that $a > 0$.

If a is negative a similar argument shows that $a = c = -1$.

(3) $a|b$ implies $b = ka$, for some integer k.
$c|d$ implies $d = lc$, for some integer l.
So $bd = ka \cdot lc = (kl)ac$, whence $ac|bd$.

(4) $a|b$ implies $b = ka$, for some integer k.
$b|c$ implies $c = lb$, for some integer l.
So $c = (lk)a$, whence $a|c$.

(5) $a|b$ implies $b = ka$, for some integer k.
$b|a$ implies $a = lb$, for some integer l.
So $ab = (kl)\, ab$, giving $kl = 1$. This occurs if and only if $k = l = \pm 1$, as in (2), whence $a = \pm b$. ▲

SAQ 11 **B** page 29, Problems 2.2, number 2.

SOLUTION TO SAQ 11 (a) Since $a|b$ there exists an integer k such that $b = ak$. But then $bc = a(kc)$ shows that $a|bc$, by Definition 2-1.

(b) Since $a|b$ and $a|c$ there exist integers k and l such that $b = ak$ and $c = al$. But then $bc = a^2(kl)$, showing that $a^2|bc$.

(c) If $a|b$ then $b = ka$, for some integer k, and $bc = k(ac)$ shows that $ac|bc$. On the other hand, if $ac|bc$ then $bc = l(ac)$ for some integer l. Since $c \neq 0$ it can be cancelled from the two sides of the equation giving $b = la$; that is, $a|b$. ■

We now encounter the greatest common divisor of two integers.

READ B from page 24, line -7 to page 27, line 3.

So now we have seen that for given integers a and b, not both zero, the set of all linear combinations of a and b is precisely the set of all multiples of $\gcd(a,b)$ and, in particular, the least positive member of this set is $\gcd(a,b)$ itself.

To illustrate our results so far let us look at

EXAMPLE 4 **B** page 30, Problems 2.2, number 13.

Part (a) is straightforward. If there exist integers x and y such that $c = ax + by$ then, by the Corollary, c is a multiple of $\gcd(a,b)$. That is, $\gcd(a,b)|c$. On the other hand, if $\gcd(a,b)|c$, then $c = k \cdot \gcd(a,b)$ for some integer k, and since there are integers x, y such that $ax + by = \gcd(a,b)$ we have $c = k \cdot \gcd(a,b) = kx \cdot a + ky \cdot b$.

Part (b) is also a consequence of the Corollary. Let $ax + by = \gcd(a,b)$, where $\gcd(a,b) = d$. Then, since $d|a$, $\frac{a}{d}$ is an integer, and similarly, $\frac{b}{d}$ is an integer. Dividing through the given equation by d gives

$$\left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y = 1.$$

So 1, the least positive integer, is a linear combination of x and y and is therefore the greatest common divisor of x and y.

SAQ 12 Use the Corollary on **B** page 26 to solve **B** page 30, Problems 2.2, number 11.

SOLUTION TO SAQ 12 Since $ax + by = (-a)(-x) + by$, it follows that every linear combination of a and b is a linear combination of $-a$ and b, and conversely. Therefore the smallest positive linear combination of a and b is the smallest positive linear combination of $-a$ and b. By the Corollary, $\gcd(a,b) = \gcd(-a,b)$.

The other two parts follow similarly from observing that

$$ax + by = ax + (-b)(-y) = (-a)(-x) + (-b)(-y). \quad \blacksquare$$

The final reading passage of the section focusses on pairs of integers whose greatest common divisor is 1, and leads to further important divisibility properties.

READ B from page 27, line 5 to the end of Section 2.2.

NOTE *Page 29, line 4*

There are many 'algebraic systems' which have a natural concept of division. For instance, in the set of all polynomials with integer coefficients we say $(3x^2 - 2x + 4)|(3x^3 + x^2 + 2x + 4)$ since

$$3x^3 + x^2 + 2x + 4 = (x + 1)(3x^2 - 2x + 4).$$

Or, in the Gaussian integers (that is, the set $\{a + ib\colon a, b \text{ are integers}, i^2 = -1\}$) we have $(1 + 2i)|(6 + 2i)$ since $6 + 2i = (1 + 2i)(2 - 2i)$.

But in neither of these systems can we generalize **B**'s Definition 2-2, since in neither system do we have a notion of 'greatest'. Which is the bigger of $2x + 1$ and $3x - 5$? Which is the bigger of $3 + 2i$ and $2 - 3i$? However, properties (1) and (2) of Theorem 2-6 make sense in each of these systems, and so can be taken as a definition of greatest common divisor. (A minor problem ensues, because the greatest common divisor so defined is not unique—but that's another story!) ▲

As an illustration of the use of Theorem 2-4 let us look at

EXAMPLE 5 **B** page 30, Problems 2.2, number 16, parts (a) and (c).

(a) To show that $\gcd(a, bc) = 1$, Theorem 2-4 tells us that it suffices to find integers r and s such that $ar + (bc)s = 1$. Now we are given that $\gcd(a, b) = \gcd(a, c) = 1$ and so, by Theorem 2-4 again, we know that there are integers x, y, u and v such that $ax + by = 1$ and $au + cv = 1$. Therefore, multiplying these equations together,

$$\begin{aligned} 1 &= (ax + by)(au + cv) \\ &= a(aux + cvx + byu) + bc(yv) \end{aligned}$$

so that 1 is a linear combination of a and bc, as required.

(c) To establish that $\gcd(ac, b) = \gcd(c, b)$ we shall show that $\gcd(ac, b) \leq \gcd(c, b)$, and that $\gcd(c, b) \leq \gcd(ac, b)$.

Given that $\gcd(a, b) = 1$ we have $ax + by = 1$ for some integers x and y. Multiplying by c,

$$(ac)x + b(yc) = c,$$

shows that c is a linear combination of ac and b and hence, by the Corollary to Theorem 2-3, a multiple of $\gcd(ac, b)$. That is, $\gcd(ac, b)|c$. But $\gcd(ac, b)|b$, by the definition of greatest common divisor, and so being a common divisor of b and c, $\gcd(ac, b) \leq \gcd(b, c)$

On the other hand, $\gcd(b, c)$ divides c (and therefore ac) and b, and so is a common divisor of ac and b. That is, $\gcd(b, c) \leq \gcd(ac, b)$.

SAQ 13 Use the result of Theorem 2-4 to prove the following.

(i) If $\gcd(a, b) = 1$ and $c|a$, then $\gcd(b, c) = 1$.

(ii) If $\gcd(a, b) = 1$ then $\gcd(a, a + b) = 1$.

SOLUTION TO SAQ 13

(i) Since $\gcd(a, b) = 1$ we can write $ax + by = 1$, for some integers x and y. But $c|a$, and so $a = kc$, for some integer k. Combining these two equations gives

$$c(kx) + by = 1,$$

so that $\gcd(b, c) = 1$, by Theorem 2-4.

(ii) Again $\gcd(a, b) = 1$ and so $ax + by = 1$. This equation can be rearranged as $a(x - y) + (a + b)y = 1$, which expresses 1 as a linear combination of a and $a + b$, as required. ■

1.6 The Euclidean Algorithm

In the previous section we discovered a number of properties of the greatest common divisor, but so far we have developed no techniques for actually calculating the greatest common divisor of two given integers. If all divisors of the two integers are easily calculated then inspection will suffice, but for handling larger integers we need an alternative approach.

XAMPLE 6 Suppose we wish to calculate gcd (1729, 703). Applying the Division Algorithm (dividing 1729 by 703), we find that $1729 = 2 \cdot 703 + 323$. From this equation we see that any common divisor of 703 and 1729 also divides 323. On the other hand, any common divisor of 323 and 703 also divides 1729. It therefore follows that the set of all common divisors of 1729 and 703 is the same as the set of all common divisors of 703 and 323; in particular, $\gcd(1729, 703) = \gcd(703, 323)$.

This has considerably reduced the size of the integers in our original problem, so it seems a good idea to repeat the procedure to reduce them still further. Let's see what happens.

$$\begin{aligned}
1729 &= 2\cdot 703 + 323 & \gcd(1729, 703) &= \gcd(703, 323)\\
703 &= 2\cdot 323 + 57 & \gcd(703, 323) &= \gcd(323, 57)\\
323 &= 5\cdot 57 + 38 & \gcd(323, 57) &= \gcd(57, 38)\\
57 &= 1\cdot 38 + 19 & \gcd(57, 38) &= \gcd(38, 19)\\
38 &= 2\cdot 19 + 0 & \gcd(38, 19) &= 19
\end{aligned}$$

To get from one line to the next in the above, we have applied the Division Algorithm to the previous divisor divided by the previous remainder. The last non-zero remainder is the greatest common divisor that we were looking for.

SAQ 14 Apply the above procedure to find gcd(306, 657).

SOLUTION TO SAQ 14

$657 = 2\cdot 306 + 45$

$306 = 6\cdot 45 + 36$

$45 = 1\cdot 36 + 9$

$36 = 4\cdot 9 + 0$

$\gcd(657, 306) = 9$ ■

This method of obtaining greatest common divisors, by repeated application of the Division Algorithm, is known as the Euclidean Algorithm. The next reading section proves that the Euclidean Algorithm does produce greatest common divisors and sets up the machinery for finding integer solutions x and y to equations of the form $ax + by = c$.

READ B from the beginning of Section 2.3 on page 31 to page 35, line 6.

SAQ 15 **B** page 37, Problems 2.3, number 2, parts (a) and (d).

SOLUTION TO SAQ 15

(a) $72 = 1\cdot 56 + 16$

$56 = 3\cdot 16 + 8$

$16 = 2\cdot 8 + 0$

$\therefore \gcd(56, 72) = 8$

Reversing these steps,

$8 = 56 - 3\cdot 16$

$8 = 56 - 3(72 - 1\cdot 56)$

$8 = 4\cdot 56 + (-3)\cdot 72$

(d) $2378 = 1\cdot 1769 + 609$

$1769 = 2\cdot 609 + 551$

$609 = 1\cdot 551 + 58$

$551 = 9\cdot 58 + 29$

$58 = 2\cdot 29 + 0$

$\therefore \gcd(1769, 2378) = 29$

$29 = 551 - 9\cdot 58$

$29 = 551 - 9(609 - 1\cdot 551)$

$29 = (-9)\cdot 609 + 10(1769 - 2\cdot 609)$

$29 = 10\cdot 1769 - 29(2378 - 1\cdot 1769)$

$29 = 39\cdot 1769 + (-29)\cdot 2378$ ■

The remainder of **B** Section 2.3 introduces the closely allied concept of the least common multiple of two integers.

READ B from page 35, line 7 to the end of Section 2.3.

SAQ 16 Find $\text{lcm}(306, 657)$.

SOLUTION TO SAQ 16 Since $\gcd(306, 657) = 9$ by SAQ 14, $\text{lcm}(306, 657) = \dfrac{306 \cdot 657}{9} = 22338$. ■

1.7 The Linear Diophantine Equation

The term Diophantine equation is used to signify an algebraic equation in one or (usually) more variables which is to be solved in the set of integers. As this course progresses, we shall encounter numerous Diophantine equations, and *Unit 8* is devoted to looking at some of the more famous problems in this area. In this section we introduce the simplest non-trivial Diophantine equation: the linear equation in two variables. Its presence is appropriate at this point because of the role played in its solution by the greatest common divisor of the coefficients of the two variables. However, it should be mentioned that the solution of the linear Diophantine equation that we obtain in Theorem 2-9 is of more theoretical importance than of practical use. We shall later find other methods of solving these equations.

READ B from the beginning of Section 2.4 on page 38, to the foot of page 39.

SAQ 17 Which of the following Diophantine equations have solutions? (We are not asking you to solve them at this stage.)

(i) $54x + 21y = 906$

(ii) $45x + 105y = 200$

(iii) $201x - 101y = 1$

SOLUTION TO SAQ 17 We test whether the greatest common divisor of the coefficients of x and y divides the right-hand side.

(i) $\gcd(54, 21) = 3 \cdot \gcd(18, 7) = 3$, and $3 | 906$ so the equation has solutions.

(ii) $\gcd(45, 105) = 3 \cdot \gcd(15, 35) = 15 \cdot \gcd(3, 7) = 15$, and $15 \nmid 200$ so the equation has no solutions.

(iii) From the Euclidean Algorithm:

$$201 = 1 \cdot 101 + 100$$
$$101 = 1 \cdot 100 + 1$$
$$100 = 100 \cdot 1$$

We see that $\gcd(-101, 201) = \gcd(101, 201) = 1$, and the equation has solutions. ■

We have seen that the equation $ax + by = c$ has solutions if and only if $d | c$, where $d = \gcd(a, b)$. Suppose we have a solvable equation in which $d \geq 2$. In this case, the coefficients a, b and c have a common divisor d which could be cancelled from the two sides of the equation. For instance, on page 39 **B** considers the equation $3x + 6y = 18$, where $\gcd(3, 6) = 3$, which divides 18. Dividing by 3, we could consider instead the equation $x + 2y = 6$, which has the same solution set.

An alternative way of looking at the solvability of the equation $ax + by = c$ is to cancel out all common factors of a, b and c to obtain an equation $a'x + b'y = c'$ which has the same solution set. This equation has a solution if and only if

$\gcd(a', b')$ divides c', but, as all common factors have been cancelled, no non-trivial divisor of a' and b' can divide c'. So for solutions we must have $\gcd(a', b') = 1$.

In the next reading passage we extend the result of the solvability of $ax + by = c$ to show how, from any one solution, all other solutions can be obtained. In Theorem 2-9, **B** continues to look at the case where $\gcd(a, b, c) = d$ may exceed 1 (which will be needed in *Unit 3*): he summarizes the important case $d = 1$ in the Corollary on page 42.

READ B from the top of page 40 to the end of Section 2.4.

SAQ 18 **B** page 43, Problems 2.4, number 2, parts (b) and (c).

SAQ 19 Find an integer solution of $201x - 101y = 1$ which satisfies $200 < x < 300$.

SAQ 20 If I spend exactly £10 to buy some 8p and some 10p stamps so that the difference in number between the two kinds of stamps bought is as small as possible, how many stamps have I bought?

SOLUTION TO SAQ 18 (b) $54x + 21y = 906$

We have seen in SAQ 17 that $\gcd(54, 21) = 3$, and as $3|906$, the equation has solutions. We first (optionally) divide through by 3, obtaining the equation $18x + 7y = 302$. Reversing the steps in the Euclidean Algorithm we next express $\gcd(18, 7) = 1$ as a linear combination of 18 and 7.

$$\left.\begin{aligned} 18 &= 2 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}\right\} \iff \left\{\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) = 2 \cdot 4 - 7 \\ &= 2 \cdot (18 - 2 \cdot 7) - 7 \\ &= 2 \cdot 18 + (-5) \cdot 7 \end{aligned}\right.$$

Now multiplying by 302 gives

$$302 = 604 \cdot 18 + (-1510) \cdot 7$$

so that $x_0 = 604$, $y_0 = -1510$ is one solution. The other solutions are given by

$$\{x = 604 + 7t, y = -1510 - 18t : t \text{ any integer}\}.$$

We require that x and y are both positive.

For $x > 0$, $604 + 7t > 0$. That is, $t \geq -86$.

For $y > 0$, $-1510 - 18t > 0$. That is, $t \leq -84$.

There are therefore three solutions in positive integers:

(i) $t = -86$, giving $x = 2$, $y = 38$;

(ii) $t = -85$, giving $x = 9$, $y = 20$;

(iii) $t = -84$, giving $x = 16$, $y = 2$.

(c) $123x + 360y = 99$

This equation clearly has no *positive* solutions. For if $x \geq 1$ and $y \geq 1$ then the left-hand side has least value 483. ■

SOLUTION TO SAQ 19 $201x - 101y = 1$

We have already seen that this equation has solutions and, since $2 \cdot 101 - 201 = 1$, it is not unreasonable to 'spot' a first solution $201(-1) - 101(-2) = 1$. By Theorem 2-9 the general solution is given by

$$\{x = -1 - 101t, y = -2 - 201t : t \text{ any integer}\}.$$

In order to satisfy the condition $200 < x < 300$ we require

$$200 < -1 - 101t < 300$$

i.e.

$$201 < -101t < 301$$

which is clearly satisfied only by $t = -2$. So the answer is

$$x = -1 + 101 \cdot 2 = 201$$

$$y = -2 + 201 \cdot 2 = 400. \quad \blacksquare$$

SOLUTION TO SAQ 20 Let x be the number of 8p stamps and y the number of 10p stamps. Then $8x + 10y = 1000$. Since $\gcd(8, 10) = 2$ and $2|1000$, we divide by 2 obtaining the equivalent equation $4x + 5y = 500$, known to have solutions.

Indeed, some solutions are easily spotted, for instance $x = 0$ and $y = 100$. Using this particular solution, Theorem 2-9 gives us the general solution:

$$\{x = 0 + 5t, y = 100 - 4t : t \text{ any integer}\}.$$

Now we wish to minimize $|x - y|$, i.e. $|9t - 100|$. This is done by choosing t to be the nearest integer to $\frac{100}{9}$, namely $t = 11$. The corresponding solution is

$x = 55, y = 56,$

and the total number of stamps bought is 111. $\blacksquare$

1.8 Problem Solving

We round off this unit with a short section on problem solving. The problems listed below are, by and large, more difficult than corresponding SAQs in the text and are different in style, being investigatory. Three of the problems ask you to discover the result in question before attempting to prove it. The section is accompanied by a tape cassette in which we discuss the problems and give you guidance on how to go about solving them.

The sole objective of this, and a similar sections in *Unit 3*, is to help you develop skill in problem solving.

If you feel confident that you can solve the problems below without the help of the tape then fire away. You will find formal solutions to these problems at the end of the Exercise Booklet. Otherwise:

START THE TAPE WHEN YOU ARE READY

ROBLEM 1 Investigate values of $n!$ and n^3 for small values of n. Make a conjecture about the relative sizes of $n!$ and n^3 and prove your result.

ROBLEM 2 (a) Show that 2 divides $n^5 - n$ for all integers n.

(b) Investigate $n^5 - n$ for small values of n and make a conjecture about the largest integer which divides $n^5 - n$ for all integers n.

(c) Prove your conjecture.

ROBLEM 3 (a) Find all integer solutions of the simultaneous system of equations below.

$$3x + 7y + 9z = 300$$

$$2x + 3y + 5z = 167$$

(b) For which of these solutions are x, y and z all positive?

PROBLEM 4 (a) Why does the Diophantine equation

$$6x + 15y - 18z = 100$$

have no solutions?

(b) What condition will ensure that the Diophantine equation

$$ax + by + cz = k$$

has no solutions? Prove your result.

(c) (Much harder.) What conditions will ensure that the equation in (b) has integer solutions? Prove your result.

1.9 Summary

In this unit we have covered Chapters 1 and 2 of **B**. Chapter 1, the historical section apart, revised two familiar ideas; proof by mathematical induction in its various forms, and the Binomial Theorem, whose coefficients we shall encounter from time to time in the course.

The first three sections of Chapter 2 form the real foundation of the whole of this course. Many of the ideas that we met there—the Division and Euclidean Algorithms, greatest common divisor and least common multiple—were quite possibly not new to you, but the simple divisibility properties of the integers that they entail are central to the whole of the course, and these ideas must be grasped now.

The final section of Chapter 2 investigated the linear Diophantine equation and showed how, when the equation is solvable, to reach a solution by means of the Euclidean Algorithm.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

UNIT 2
PRIMES AND THEIR DISTRIBUTION

2.0 Introduction

This unit comprises Chapter 3 and the first section of Chapter 13 of **B**. The unit is mainly concerned with properties of the prime numbers:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots,$$

that is, those positive integers which have exactly two positive divisors; the integer itself and 1. The major result of the unit, the Fundamental Theorem of Arithmetic, tells us that every integer greater than 1 can be written as a product of primes and that this product is unique apart from the order in which the primes are written. For example, 12 may be written as $3 \cdot 2 \cdot 2$ or $2 \cdot 3 \cdot 2$, or $2 \cdot 2 \cdot 3$, but no other factorizations of 12 into a product of primes are possible.

The fact that the primes are the 'building blocks' from which all natural numbers are made certainly accounts for their importance. It does not, however, account for the fascination which they have exerted—and continue to exert. Many of the most famous problems in mathematics, both solved and unsolved, involve prime numbers and their distribution. How many primes are there? Is there a largest prime? Is there a formula for generating all prime numbers? How many primes p are there so that $p + 2$ is also prime? Can every even integer greater than 2 be written as the sum of two primes? This unit will provide answers to some of these questions and will discuss others which, despite considerable numerical evidence to support their validity, remain unsolved despite years of continual assault upon them.

In Section 2.4 we introduce and discuss what is perhaps the most intriguing sequence of integers in mathematics—the Fibonacci sequence. As well as being of interest for its own sake, the Fibonacci sequence will enable us to gain practice in using results and techniques developed elswhere in the first two units; in particular, divisibility properties which, by this stage, include the divisibility properties for primes.

2.1 The Fundamental Theorem of Arithmetic

In this section we introduce the primes and give a proof of the fact that every integer greater than 1 can be expressed as a product of primes in a unique way (apart from their order).

READ B Section 3.1, page 46, as far as page 47, line -4.

NOTES (i) *Page 46, line 14*

Many students are reluctant to abandon the mistaken belief that 1 is a prime. But, as **B** says, we do not classify 1 as either prime or composite. For, if we classify it as prime then we can express integers as products of primes in many different ways; for instance,

$$6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 2 \cdot 3 \cdot 1$$

and the Fundamental Theorem of Arithmetic is lost. On the other hand, we wish to reserve the description composite for those positive integers which can be written as a product of two or more primes.

(ii) *Page 47, line 6*

If the concept of a prime is not new to you, you may feel that Theorem 3-1 and its Corollaries are so obvious that they hardly need proving. However fundamental primes may be, the theorems about them do not spring full-grown out of Definition 3-1 alone. Here for instance, following the logical development of **B**, we call upon Euclid's Lemma which was proved previously without reference to primes. ▲

To illustrate the use of these results let us look at

XAMPLE 1 Let p be a prime and a and b be integers. Prove

(a) if $p|a^n$ then $p^n|a^n$;

(b) if $\gcd(a, b) = p$ then $\gcd(a^n, b^n) = p^n$.

(a) Using Corollary 1 with $a_1 = a_2 = \cdots = a_n$, we deduce immediately that if $p|a^n$ then $p|a$. So writing $a = pr$, for some integer r, and raising both sides of this equation to power n gives $a^n = p^n r^n$, which tells us that $p^n|a^n$.

(b) As $\gcd(a, b) = p$, there exist integers r and s such that $a = pr$ and $b = ps$, with $\gcd(r, s) = 1$. But then

$$\begin{aligned}\gcd(a^n, b^n) &= \gcd(p^n r^n, p^n s^n)\\ &= p^n \gcd(r^n, s^n) \qquad \text{(by Theorem 2-7, } \mathbf{B} \text{ page 34)}\end{aligned}$$

and it remains to show that $\gcd(r^n, s^n) = 1$.

Suppose $q|\gcd(r^n, s^n)$, where q is a prime. Then $q|r^n$ and $q|s^n$. As we saw in part (a), this implies that $q|r$ and $q|s$, so that $q|\gcd(r, s)$. But $\gcd(r, s) = 1$, and so no such prime q can exist, and $\gcd(r^n, s^n) = 1$.

SAQ 1 **B** page 51, Problems 3.1, number 7.

SAQ 2 Given that p_1 and p_2 are distinct primes such that their product $p_1 p_2$ divides a^n, prove that $(p_1 p_2)^n|a^n$.

OLUTION TO SAQ 1 By Corollary 1, any prime dividing 50! must divide one of the numbers in the sequence 1, 2, 3,……, 49, 50, and hence cannot exceed 50. On the other hand, each prime not exceeding 50 occurs in this sequence and so certainly divides 50! The question therefore boils down to finding all the primes not exceeding 50. These are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

(A list of primes less than 10,000 is given in Tables 2 and 3 in the Appendices of **B**, and a systematic method of finding primes is described in Section 2.2 of this unit.) ■

OLUTION TO SAQ 2 Since $p_1 p_2|a^n$ we know that $p_1|a^n$ and $p_2|a^n$. As in part (a) of Example 1, this gives $p_1|a$ and $p_2|a$. Now $\gcd(p_1, p_2) = 1$. Therefore, appealing to Theorem 2.4, Corollary 2, $p_1 p_2|a$. Finally, writing $a = p_1 p_2 b$ gives $a^n = (p_1 p_2)^n b^n$, and so $(p_1 p_2)^n|a^n$, as required. ■

READ B from page 47, line −3 to page 50, line 5.

NOTE *Page 49, line −8*

The literal meaning of the word canonical is standard (or regular). In mathematics, when some quantity or formula is capable of being expressed in a variety of ways it is often convenient to choose a particular presentation as the standard one, i.e. the canonical one. The canonical form for expressing an integer greater than 1 as a product of primes is the one in which the prime factors are placed in ascending order and multiple occurrences of the same prime are collected together and written as a power. ▲

To illustrate the canonical form let us look at

XAMPLE 2 **B** page 52, Problems 3.1, number 15.

Firstly let us suppose that $a > 1$ is a square, say $a = b^2$, where since $a > 1$ we may choose $b > 1$. Let the canonical form for b be

$$b = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

Then

$$a = b^2 = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^2 = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r}$$

which is in canonical form (the primes are in ascending order with multiple occurrences collected together), with all the exponents even.

On the other hand, if all the exponents in a are even then

$$\begin{aligned} a &= p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r} \\ &= (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^2 \end{aligned}$$

is certainly a square.

SAQ 3 **B** page 51, Problems 3.1, number 12.

SAQ 4 Prove that an integer $a > 1$ is an nth power if and only if in the canonical form of a all the exponents are divisible by n.

SAQ 5 **B** page 50, Problems 3.1, number 3.

SOLUTION TO SAQ 3

$1234 = 2 \cdot 617$

$10140 = 2^2 \cdot 3 \cdot 5 \cdot 13^2$

$36000 = 2^5 \cdot 3^2 \cdot 5^3$. ■

SOLUTION TO SAQ 4

Let $a = b^n$ where $b = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is in canonical form.

Then

$$a = b^n = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^n = p_1^{nk_1} p_2^{nk_2} \cdots p_r^{nk_r}$$

has each exponent divisible by n.

On the other hand, if a has canonical form with each exponent divisible by n, then

$$a = p_1^{nk_1} p_2^{nk_2} \cdots p_r^{nk_r} = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^n$$

is certainly an nth power. ■

SOLUTION TO SAQ 5

(a) Let $p = 3n + 1$. As 2 is not of the form $3n + 1$, p is an odd prime. Hence $p - 1 = 3n$ is even, and so $2|3n$, from which it follows that $2|n$. Writing $n = 2m$ gives $p = 6m + 1$ as required.

(b) Let $3n + 2 = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ be its canonical form, so that the primes dividing $3n + 2$ are $p_1, p_2, \ldots, p_r$ where $r \geq 1$. Now $3n + 2$ is not divisible by 3 and so none of p_i is 3. Therefore each prime divisor of $3n + 2$ is of one of the forms $3k + 1$ or $3k + 2$.

The identity

$$(3r + 1)(3s + 1) = 3(3rs + r + s) + 1$$

shows that the product of two numbers of the form $3k + 1$ is of the same form. It follows, by induction, that any product of numbers of the form $3k + 1$ is itself of that same form. Hence, if each p_i is of the form $3k + 1$ then so too is $3n + 2$, which is not the case. We conclude that at least one of the prime factors p_i of $3n + 2$ is of the form $3k + 2$.

(c) Using the hint,

$$n^3 - 1 = (n - 1)(n^2 + n + 1)$$

expresses the prime $n^3 - 1$ as a product of two positive factors. The uniqueness of factorization tells us that this is possible only if one of the factors on the right-hand side is equal to 1. Now $n > 1$ (since $n^3 - 1$ is a prime), and so $n^2 + n + 1 > 3$. The only remaining possibility is that $n - 1 = 1$, i.e. $n = 2$, giving $n^3 - 1 = 7$.

(d) Suppose $3p + 1$ is a square, say $3p + 1 = n^2$. Then

$$3p = n^2 - 1 = (n - 1)(n + 1).$$

As $3p + 1 \geq 7$ we know that $n > 2$ so that neither factor on the right of the above equation is equal to 1. By uniqueness of factorization we therefore have either $3 = n - 1$ and $p = n + 1$, or $3 = n + 1$ and $p = n - 1$. These give respectively $n = 4$, $p = 5$ and $n = 2$, $p = 1$, and the first case is the only possibility. ■

If the prime factorization of an integer is given, it is a simple matter to obtain all divisors of that integer. For example, spend a minute or two thinking about the prime factorizations of divisors of the integer $252 = 2^2 \cdot 3^2 \cdot 7$ and, without calculating them, see if you can formulate a conjecture about the set of all divisors of 252.

You should quickly appreciate that if d is a divisor of 252 then d can involve only the primes 2, 3 and 7. What is more, since $2^3 \nmid 252$, $3^3 \nmid 252$ and $7^2 \nmid 252$, the exponent in d of each of these primes cannot exceed the corresponding exponent in 252. From these facts we draw the conclusion that the divisors of 252 are the integers $2^r \cdot 3^s \cdot 7^t$ where $r = 0$, 1 or 2, $s = 0$, 1 or 2 and $t = 0$ or 1. These 18 integers (3 choices for r, 3 choices for s and 2 choices for t give a total of $3 \cdot 3 \cdot 2$ choices, and by uniqueness of factorization the resulting numbers are distinct) are the only divisors of 252. Notice that they include 1 ($r = s = t = 0$) and 252 itself ($r = s = 2$, $t = 1$).

Let us turn to the general situation. Let

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

be an integer greater than 1 given in canonical form. Extending the observations of the above example we claim that the set of all divisors of a is the set of integers

$$\{p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} : 0 \leq l_i \leq k_i \text{ for } i = 1, 2, \ldots, r\}.$$

Certainly each integer in this set is a divisor of a, since

$$a = p_1^{k_1}\, p_2^{k_2} \cdots p_r^{k_r} = (p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r})\, p_1^{k_1 - l_1}\, p_2^{k_2 - l_2} \cdots p_r^{k_r - l_r}$$

and so our task now is to show that these, which are distinct by unique factorization, are the only divisors of a.

Let d be any divisor of a and let p be a prime factor of d. Since $p|d$ and $d|a$ we know that $p|a$ and so, by Theorem 3-1, Corollary 2, $p = p_i$ for some i in the range $1 \leq i \leq r$. As the possible prime factors of d are $p_1, p_2, \ldots, p_r$ it now follows that we can write $d = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$, where each l_i is a non-negative integer.

Finally, to show $l_i \leq k_i$ we utilize the fact that $d|a$ and in particular that $p_i^{l_i}|a$. As the primes $p_1, p_2, \ldots, p_r$ are distinct, $p_1 \nmid p_2^{k_2} p^{k_3} \cdots p_r^{k_r}$, for otherwise we contradict Theorem 3-1, Corollary 2. It follows that $\gcd(p_1^{l_1}, p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}) = 1$. Applying Euclid's Lemma, $p_1^{l_1}|p_1^{k_1}(p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r})$ gives $p_1^{l_1}|p_1^{k_1}$, which requires $l_1 \leq k_1$. The same argument can be used to establish $l_2 \leq k_2, \ldots, l_r \leq k_r$, as required.

SAQ 6 (a) Let $a = 3^3 \cdot 5 \cdot 17^2$ and $b = 2 \cdot 3^2 \cdot 7 \cdot 17^4$.

(i) How many positive divisors does a have?

(ii) List the common divisors of a and b.

(iii) Determine $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$.

(b) In general, if a and b are integers whose prime factorizations are given, how do you obtain $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$? Prove your result.

SOLUTION TO SAQ 6

(a) (i) The divisors of a are the integers $3^r \cdot 5^s \cdot 17^t$ where $0 \le r \le 3$, $0 \le s \le 1$ and $0 \le t \le 2$, of which there are $4 \cdot 2 \cdot 3 = 24$.

(ii) The common divisors of a and b are

$$1,\ 3,\ 3^2,\ 17,\ 3\cdot 17,\ 3^2\cdot 17,\ 17^2,\ 3\cdot 17^2 \text{ and } 3^2\cdot 17^2.$$

(iii) $\gcd(a,b) = 3^2 \cdot 17^2$

$$\begin{aligned}\operatorname{lcm}(a,b) &= \frac{ab}{\gcd(a,b)}\\ &= \frac{3^3\cdot 5\cdot 17^2\cdot 2\cdot 3^2\cdot 7\cdot 17^4}{3^2\cdot 17^2}\\ &= 2\cdot 3^3\cdot 5\cdot 7\cdot 17^4.\end{aligned}$$

(b) Let $p_1, p_2, \ldots, p_r$ be the primes which divide either a or b. Then we write

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad\text{and}\quad b = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$$

where exponents may be zero. For example, $k_i = 0$ if $p_i | b$ but $p_i \nmid a$.

A divisor of a is an integer

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

where $0 \le \alpha_i \le k_i$ for each $i = 1, 2, \ldots, r$. For d also to divide b we require $\alpha_i \le l_i$, for each $i = 1, 2, \ldots, r$. Combining these two conditions, d is a common divisor of a and b if and only if $0 \le \alpha_i \le \min\{k_i, l_i\}$ (the smaller of k_i and l_i) for each $i = 1, 2, \ldots, r$. Therefore,

$$\gcd(a,b) = p_1^{\min\{k_1,l_1\}} p_2^{\min\{k_2,l_2\}} \cdots p_r^{\min\{k_r,l_r\}}.$$

In words, we obtain the prime factorization of gcd (a, b) by raising each prime to the power which is the smaller of its exponents in a and b.

$$\begin{aligned}\operatorname{lcm}(a,b) &= \frac{ab}{\gcd(a,b)}\\ &= \frac{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\, p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}}{p_1^{\min\{k_1,l_1\}} \cdots p_r^{\min\{k_r,l_r\}}}\\ &= p_1^{k_1+l_1-\min\{k_1,l_1\}} \cdots p_r^{k_r+l_r-\min\{k_r,l_r\}}.\end{aligned}$$

For any two numbers k and l, $k + l - \min\{k, l\} = \max\{k, l\}$ (the larger of k and l). Therefore

$$\operatorname{lcm}(a,b) = p_1^{\max\{k_1,l_1\}} p_2^{\max\{k_2,l_2\}} \cdots p_r^{\max\{k_r,l_r\}}.$$

In words, we obtain the prime factorization of lcm (a, b) by raising each prime to the power which is the larger of its exponents in a and b.

As a further illustration of these results, if $a = 3^3 \cdot 5^3 \cdot 11 \cdot 19$ and $b = 2 \cdot 3^2 \cdot 7 \cdot 11^2$ then

$$\gcd(a,b) = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^1 \cdot 19^0 = 3^2 \cdot 11$$

(where for each prime occurring in a or b we take the smaller exponent) and

$$\operatorname{lcm}(a,b) = 2 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 11^2 \cdot 19$$

(where the larger exponent is taken). ■

READ B from page 50, line 6 to the end of Section 3.1.

There are many different forms that the proof of Theorem 3-3 can take. The usual elementary proof observes that if $a^2 = 2b^2$ then a^2 is even which means that a must be even (as the square of an odd integer is odd). Replacing a by $2c$ gives $2c^2 = b^2$, and the same argument now tells us that b is even. So 2 is a common factor of a and b, contradicting the assumption that $\gcd(a, b) = 1$.

The advantage of the proof given in **B** is its generality. For if N is a positive integer which is not a perfect square, the same proof (replacing 2 by N as appropriate) shows that $\sqrt{N}$ is irrational.

The uniqueness of prime factorization provides us with a third proof. Suppose $a^2 = 2b^2$. We know from SAQ 4 that each prime exponent in a^2 and in b^2 is even. Focussing upon the prime 2, its exponent in a^2 is even whilst its exponent in $2b^2$ is odd, a contradiction. Hence $a^2 = 2b^2$, (i.e. $a/b = \sqrt{2}$) is impossible.

SAQ 7 Prove that if the integer $c > 1$ is not the nth power of an integer then $\sqrt[n]{c}$, the nth root of c, is not a rational number.

SOLUTION TO SAQ 7 Suppose that $\sqrt[n]{c}$ is the rational number a/b. Then $a^n = cb^n$. By SAQ 4 we know that each prime divisor of a^n and b^n has exponent divisible by n and that c (since it is not an nth power) has at least one prime divisor, say p, whose exponent is not divisible by n. So the exponent of p in a^n is divisible by n whilst the exponent of p in cb^n is not divisible by n. This contradicts the uniqueness of prime factorization. ■

2.2 The Sieve of Eratosthenes

As we have remarked, Tables 2 and 3 at the end of **B** give a complete list of primes less than 10,000. How would one go about compiling such a table? In the solution to SAQ 1 you used all the primes less than 50 and maybe you found them by applying the definition, taking each integer in turn and trying to find factors by dividing by all smaller positive integers. If so, you will realize that such a crude method would be very time consuming.

Fortunately, there is a rather more efficient way of testing for primality and for producing lists of primes, and both techniques are discussed in this section. Finally, we settle one of the problems posed in the introduction to the unit by proving that there are infinitely many primes.

READ B Section 3.2 from page 52 as far as page 54, line −12.

SAQ 8 **B** page 57, Problems 3.2, number 1.

SAQ 9 **B** page 57, Problems 3.2, number 2.

SAQ 10 **B** page 57, Problems 3.2, number 3.

SOLUTION TO SAQ 8 As $26^2 < 701 < 27^2$, we test 701 for divisibility by the primes not exceeding 26. These are 2, 3, 5, 7, 11, 13, 17, 19 and 23, and as none of them divide 701 the latter is a prime.

Similarly, $31^2 < 1009 < 32^2$, and as 1009 is not divisible by any prime ≤ 31 it is itself prime. ■

SOLUTION TO SAQ 9 Since $14 < \sqrt{200} < 15$, removing from the set of integers from 100 to 200 all the multiples of 2, 3, 5, 7, 11 and 13 leaves just the primes behind. These are:

101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151,
157, 163, 167, 173, 179, 181, 191, 193, 197, 199. ■

SOLUTION TO SAQ 10 We have seen that a composite integer n must have a divisor other than 1 which does not exceed $\sqrt{n}$. This problem is a simple extension of this result to integers having three (or more) non-trivial divisors.

Suppose $n = abc$ where $a > 1$, $b > 1$ and $c > 1$. Now if $a > \sqrt[3]{n}$, $b > \sqrt[3]{n}$ and $c > \sqrt[3]{n}$ their product abc exceeds n, which is a contradiction. Hence at least one of these divisors must be less than or equal to $\sqrt[3]{n}$, and the divisor in question has a prime divisor with the same property.

So, if $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, then n cannot be expressed as the product of three factors each exceeding 1, which means that n is the product of at most two (not necessarily distinct) primes. ■

READ B from page 54, line -11 to the end of Section 3.2.

NOTES (i) *Page 56, line 17*
In Theorem 3-5 and its proof, use is made of indices which are themselves powers, for instance $2^{2^{n-1}}$. Strictly speaking, such expressions ought to include brackets, since $a^{(b^c)}$ is not in general equal to $(a^b)^c$. For example,

$$2^{(3^4)} = 2^{81} \quad \text{but} \quad (2^3)^4 = 8^4 = 2^{12}.$$

By convention, both in **B** and elsewhere, an unbracketed expression a^{b^c} is always to be interpreted as $a^{(b^c)}$.

(ii) *Page 56, line -11*
Observe that the proof uses the Second Principle of Mathematical Induction, as the induction hypothesis assumes that $p_k \leq 2^{2^{k-1}}$ for each integer k from $k = 1$ to $k = n$. ▲

A considerably better estimate of the size of p_n than that obtained in Theorem 3-5 is $p_n \leq 2^n$. One method of proving this result is by using Bertrand's Conjecture, which states that for every positive integer $n > 1$ there is a prime p satisfying the inequality $n < p < 2n$. This conjecture was proved by Chebyshef in 1850, and although the proof is not within the scope of this course it is instructive to see how the estimate $p_n \leq 2^n$ is derived from it.

SAQ 11 Assuming Bertrand's Conjecture, use induction to show that the nth prime p_n satisfies $p_n \leq 2^n$.

SAQ 12 **B** page 57, Problems 3.2, number 7.

SOLUTION TO SAQ 11 Since $p_1 = 2 \leq 2^1$, the result $p_n \leq 2^n$ is true when $n = 1$. Assume the result is true when $n = k \geq 1$, i.e. $p_k \leq 2^k$. By Bertrand's Conjecture there is a prime p satisfying $2^k < p < 2 \cdot 2^k = 2^{k+1}$. By hypothesis, there are at least k primes not exceeding 2^k so with the existence of p there must be at least $k + 1$ primes not exceeding 2^{k+1}. That is, $p_{k+1} \leq 2^{k+1}$, completing the induction step. By the first Principle of Finite Induction $p_n \leq 2^n$ for all $n \geq 1$. ■

SOLUTION TO SAQ 12 Suppose there are only finitely many primes and let p be the largest one. Consider $N = p! + 1$ which, being greater than p, cannot be prime and so has a prime factor, q say. As p is the largest prime, $q \leq p$ and so $q \mid p!$ But $q \mid N$ and therefore $q \mid N - p!$ That is, $q \mid 1$, an obvious contradiction. ■

2.3 The Goldbach Conjecture

Having seen that there are infinitely many prime numbers, this section looks at the distribution of primes within the positive integers. There appears to be no regularity about the occurrence of primes, and having arrived at one, there is no way of predicting how far we must go to reach the next. Nevertheless, we shall see that the gaps between successive primes become arbitrarily large; there is a gap of 6 between 23 and 29, a gap of 8 between 89 and 97, and so on. On the other hand, the minimal gap of 2 between odd primes, for pairs like 11, 13 and 41, 43, occurs very frequently. The conjecture that there exist infinitely many such pairs of primes is one of the outstanding unsolved problems of number theory.

So what questions can we reasonably ask about occurrences of primes? If you look at the arithmetic progression

$$5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, \ldots$$

you will no doubt be struck by the preponderance of primes. However, no arithmetic progression

$$a,\ a + b,\ a + 2b,\ a + 3b, \ldots, \qquad a \geq 1,\ b > 0$$

can consist entirely of primes since, as we said earlier, the gap between successive primes becomes arbitrarily large, and once we have a gap of length b, i.e. b successive composite integers, the given arithmetic progression must contain one of these composites.

In fact every arithmetic progression, like the one above, with gcd $(a, b) = 1$, contains an infinite number of primes. This classical result of number theory is due to Dirichlet and, as its proof is beyond the scope of this course, we shall restrict ourselves in this section to proving two special cases of it. Later in the course, when we have more machinery at our disposal, we shall find that we can prove several more particular instances of Dirichlet's Theorem.

En route to looking at arithmetic progressions, the section interposes a discussion of Goldbach's Conjecture. Like so many other problems involving primes, this famous conjecture has overwhelming numerical evidence for its validity but still awaits a proof.

READ B Section 3.3 from page 58 as far as page 60, line 11.

NOTE *Page 59, line −3*
It is usual to denote by $\pi(n)$ the number of primes in the set $\{1, 2, \ldots, n\}$ so that, for example, $\pi(1) = 0$, $\pi(6) = 3$ and $\pi(12) = 5$. It has been shown that

$$\lim_{n \to \infty} \frac{\pi(n)}{n} = 0.$$

In the language used here we could therefore say that 'almost all' positive integers are composite. Landau might have observed that 0% of all positive integers are prime, despite there being infinitely many of them! ▲

SAQ 13 **B** page 64, Problems 3.3, number 2.

OLUTION TO SAQ 13 (a) $p(p + 2) + 1 = (p + 1)^2$.

(b) Any integer is of one of the forms $6k + r$, where $r = 0, 1, 2, 3, 4$ or 5. When r is even, $6k + r$ is even, and when $r = 3$, $6k + r$ is divisible by 3. Therefore the prime $p > 3$ must be of one of the forms $6k + 1$ or $6k + 5$. Now $p = 6k + 1$ gives $p + 2 = 6k + 3$ which is composite. We conclude that $p = 6k + 5$ and

$$p + (p + 2) = 6k + 5 + (6k + 7) = 12(k + 1).$$

COMMENT The observation that any prime greater than 3 must be of one of the forms $6k + 1$ or $6k + 5$ certainly leads to an elegant solution. But it may well be that you failed to make this observation. A simpler approach would be to start by noting that p must be of one of the forms $3k$, $3k + 1$ or $3k + 2$. For $p > 3$ and $p + 2$ to both be prime, $p = 3k + 2$ is the only possibility, and this in turn requires k to be odd. Then

$$p + (p + 2) = (3k + 2) + (3k + 4) = 6(k + 1) = 12\left(\frac{k+1}{2}\right).$$

Alternatively, the observation that any prime greater than 3 must be of one of the forms $12k + 1$, $12k + 5$, $12k + 7$ or $12k + 11$ leads to an immediate solution. ■

READ B from page 60, line 12 to page 62, line 9.

NOTE *Page 61, line −3*
The proof given in **B** that every arithmetic progression of positive integers contains infinitely many composite numbers may seem unnecessarily complicated. For every integer n, the term $a + (na)b = a(1 + nb)$ is a composite term in the progression whenever $a \neq 1$. This simpler argument breaks down, however, for those progressions with initial term $a = 1$. ▲

SAQ 14 **B** page 64, Problems 3.3, number 13.

(Hint: Assume that $q_1, q_2, \ldots, q_s$ are the only primes of the form $6k + 5$ and obtain a contradiction by showing that $6q_1 q_2 \ldots q_s - 1$ has a prime divisor of the form $6k + 5$. You will need an analogous result to the Lemma on **B** page 60.)

SAQ 15 **B** page 65, Problems 3.3, number 18, part (a).

(Interpret 'every pth term' as meaning 'every pth term from some point onwards'.)

SOLUTION TO SAQ 14 Following the lines of the proof of Theorem 3-6, we assume that there are only finitely many primes of the form $6n + 5$, and aim to derive a contradiction; call them $q_1, q_2, \ldots, q_s$. Consider the positive integer

$$N = 6q_1 q_2 \ldots q_s - 1 = 6(q_1 q_2 \ldots q_s - 1) + 5.$$

Since N is of the form $6n + 5$ it is not divisible by 2 or 3, and so (as in the solution to SAQ 13(b)) each prime divisor of N is either of form $6n + 1$ or $6n + 5$. Now the identity

$$(6n + 1)(6m + 1) = 6(6nm + n + m) + 1$$

shows that the product of two (and, consequently, any number of) integers of the form $6n + 1$ is also of that same form. But N is not of the form $6n + 1$ and so not all its prime divisors can be of that form. We conclude that there is at least one prime divisor p of N which is of the form $6n + 5$.

Finally, $p \neq q_i$, for $i = 1, 2, \ldots, s$, for otherwise $p | 6q_1 q_2 \ldots q_s - N$, i.e. $p|1$.

This contradicts the assumption that there are only finitely many primes $q_1, q_2, \ldots, q_s$ of the form $6k + 5$, and establishes an infinitude of such primes. ■

SOLUTION TO SAQ 15 Following the hint, as $\gcd(b, p) = 1$ there exist integers r and s such that $pr + bs = 1$ (by Theorem 2-4). For each integer k, positive or negative, let $n_k = kp - as$. Observe that the (double) sequence of integers

$$\ldots, n_{-2}, n_{-1}, n_0, n_1, n_2, \ldots$$

is in arithmetic progression with common difference p. Let n_t be the first positive member of this sequence. Then

$$a + n_t b,\ a + n_{t+1} b,\ a + n_{t+2} b, \ldots$$

gives every pth term of the original arithmetic progression (from some point onwards), and it remains to show that each of these is a multiple of p. Now for all k,

$$\begin{aligned} a + n_k b &= a + (kp - as)b = a + kpb - asb \\ &= a + kpb - a(1 - pr) = kpb + apr \\ &= p(kb + ar), \end{aligned}$$

completing the proof. ■

READ B from page 62, line 10 to the end of Section 3.3.

SAQ 16 Find the smallest positive integer n for which the function $f(n) = n^2 + n + 17$ takes a composite value.

LUTION O SAQ 16

$$f(n) = n^2 + n + 17 = n(n + 1) + 17,$$

and so $f(n)$ is composite when $17 | n(n + 1)$. The first time this happens is when $n = 16$, giving $f(16) = 17^2$.

Substituting $n = 1, 2, \ldots, 15$ in $f(n)$ produces the integers 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227 and 257, all of which are prime (see Table 2). So the smallest positive integer n for which $f(n)$ is composite is 16. ■

2.4 The Fibonacci Sequence

In the previous section we investigated occurrences of primes in arithmetic progressions and in sequences

$$f(1), f(2), f(3), \ldots$$

where f is a polynomial with integer coefficients. The next step along this road is to investigate occurrences of primes in recursive sequences, i.e. sequences defined by recurrence relations. We shall restrict ourselves to considering the best known of all such recursive sequences, the Fibonacci sequence:

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

which is defined by

$$u_1 = u_2 = 1; \quad u_n = u_{n-1} + u_{n-2}, n \geq 3.$$

We shall discover in this section that the members of the Fibonacci sequence, the Fibonacci numbers, have fascinating divisibility properties, although it is still an open question as to whether there are infinitely many prime Fibonacci numbers. The section will not only serve as useful revision for ideas and results of *Unit 1*, but will also illustrate the usefulness of 'congruence', which is the theme of *Unit 3*.

READ B Section 13.1 from page 286 as far as page 288, line −10.

The result just cited is not special to primes. For any positive integer n there are infinitely many Fibonacci numbers which are multiples of n and they occur equally spaced in the Fibonacci sequence. Although **B** comments that the general proof of this result is quite cumbersome, there is an elegant proof. However, this requires some understanding of congruence and we shall therefore defer it until *Unit 3*.

In fact, for each *particular* value of n the result can be demonstrated without too much difficulty. (Unfortunately, each proof is different and there is no way of deriving from them one proof which works for all positive integers n.) Let us see how we would go about showing that every fourth term of the Fibonacci sequence is divisible by 3.

We write down a new sequence obtained from the Fibonacci sequence by replacing each term by its remainder on division by 3:

$$1, 1, 2, \underline{0}, 2, 2, 1, \underline{0}, 1, 1, 2, \underline{0}, 2, 2, 1, \underline{0}, \ldots$$

By the Division Algorithm, the terms can only be 0, 1 and 2, where the 0's correspond to the terms in the Fibonacci sequence which are divisible by 3. As you can see, every fourth term so far is a zero and what we need to prove is that this pattern of zeroes continues. The essence of the argument is that we can continue the new sequence without reference to the original Fibonacci sequence. As each Fibonacci number is the sum of the preceding two, it follows that each term of our new sequence is obtained by adding the two preceding remainders and then taking the remainders on division by 3. (We shall ask you to prove a general result of this type in SAQ 17.) For example, successive terms 2 and 1 in the remainder sequence correspond to Fibonacci numbers of the forms $3k + 2$ and $3l + 1$, and the next term is $(3k + 2) + (3l + 1) = 3(k + l + 1) + 0$, which has remainder 0 on division by 3. Our observation merely states that this remainder could have been obtained directly by adding the remainders 2 and 1 and then taking the remainder of the resulting sum.

The proof is completed by observing that the remainder sequence consists of the pattern 1, 1, 2, 0, 2, 2, 1, 0 recurring indefinitely, since once a pair of successive terms are a repeat of an earlier pair the sequence must recur, each term being the sum of the two preceding terms. So every fourth term in the remainder sequence is 0 and hence every fourth term in the Fibonacci sequence is divisible by 3.

[The underlying techniques contained in the above proof are illustrative of a powerful theory which we shall develop in general in the next unit. For a given positive integer n, replacing each integer by its remainder on division by n leads to a new 'arithmetic' on the set of remainders $\{0, 1, 2, \ldots, n - 1\}$. Results in this simpler model translate into important properties of the integers themselves.]

SAQ 17 The integers a and b have remainders r_1 and r_2 when divided by the positive integer n. Show that $a + b$ and $r_1 + r_2$ have the same remainder when divided by n. (We used the special case of this result with $n = 3$ in the above argument.)

SAQ 18 Write out the sequences of remainders when the terms of the Fibonacci sequence are divided by (i) 4, (ii) 5 and (iii) 6. What conclusions can you draw about the occurrences of the multiples of these integers in the Fibonacci sequence? Justify your conclusion for case (i).

SOLUTION TO SAQ 17

Let $a = q_1 n + r_1, \quad 0 \le r_1 < n$

and $b = q_2 n + r_2, \quad 0 \le r_2 < n.$

Now let r_3 be the remainder when $r_1 + r_2$ is divided by n, i.e.

$$r_1 + r_2 = q_3 n + r_3, \quad 0 \le r_3 < n.$$

Adding the first two equations we get

$$\begin{aligned} a + b &= q_1 n + q_2 n + r_1 + r_2 \\ &= (q_1 + q_2 + q_3)n + r_3, \quad 0 \le r_3 < n. \end{aligned}$$

Hence, by uniqueness of remainder, r_3 is the remainder on dividing $a + b$ by n.

COMMENT We have confined attention here to the important case where the integer n is positive. The result is, however, true for all non-zero integers. ■

SOLUTION TO SAQ 18 (i) 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0,...

By the result of SAQ 17, each term of the remainder sequence is obtained by adding the two preceding terms and taking the remainder of this sum on division by 4. Hence, on arriving at the successive pair 1, 0 the next two terms 1, 1 are a repeat of the initial pair and so thereafter the sequence recurs. The sequence therefore consists of the pattern 1, 1, 2, 3, 1, 0 repeated indefinitely, every sixth term being 0, and consequently every sixth term of the Fibonacci sequence (and no other) is a multiple of 4.

(ii) 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1,...

The sequence consisting of the first 20 integers above recurs indefinitely and thus every fifth term of the Fibonacci sequence is divisible by 5.

(iii) 1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, 1,...

The sequence consisting of the first 24 integers above recurs, and thus every twelfth term of the Fibonacci sequence is divisible by 6. ■

READ B page 288, line −9 to page 290, line −11.

NOTES (i) *Page 289, line −9*

In order to ensure positive subscripts in identity (1) we require the condition $m \geq 2$. This however has implications for the proof of Theorem 13-2 where the use of (1) in the induction step includes the case $m = 1$. Fortunately, Theorem 13-2 is clearly true when $m = 1$ since then $u_m = 1$. An alternative way around this difficulty is to define an extra term u_0 of the Fibonacci sequence, satisfying the recurrence relation $u_2 = u_1 + u_0$, i.e. $u_0 = 0$. This now admits the case $m = 1$ in (1), and Theorem 13-2 goes through unaltered.

(ii) *Page 290, line 12*

Note that Theorem 13-2 can be expressed more succinctly as:

$$\text{if } r|s \text{ then } u_r|u_s. \quad \blacktriangle$$

SAQ 19 Use identity (1) and the values of the first twelve Fibonacci numbers given on **B** page 287 to find u_{22}, u_{23} and u_{24}. Confirm that $u_{11}|u_{22}$ and $u_8|u_{24}$.

SOLUTION TO SAQ 19 Putting $m = n = 11$ in (1) gives

$$\begin{aligned} u_{22} &= u_{10}u_{11} + u_{11}u_{12} = u_{11}(u_{10} + u_{12}) \qquad (\text{note that } u_{11}|u_{22}) \\ &= 89 \cdot (55 + 144) \\ &= 17711. \end{aligned}$$

Putting $m = 12$ and $n = 11$ in (1) gives

$$\begin{aligned} u_{23} &= u_{11}u_{11} + u_{12}u_{12} \\ &= 89^2 + 144^2 = 28657. \end{aligned}$$

Finally,

$$u_{24} = u_{23} + u_{22} = 46368$$

and

$$46368 = 2208 \cdot 21 = 2208\,u_8. \quad \blacksquare$$

READ B from page 290, line -10 to the end of Section 13.1.

NOTE *Page 292, line 4*

Having arrived at $u_{\gcd(m,n)} = u_m$, **B** concludes that $m = \gcd(m, n)$. If all the Fibonacci numbers are distinct this would be valid, but unfortunately $u_1 = u_2 = 1$. Hence the conclusion that $m = \gcd(m, n)$ can only be drawn provided $m > 2$. However, Theorem 13-3 is trivially true in the cases $m = 1$ and $m = 2$, so all is well.

This explains why the Corollary requires the hypothesis that $m > 2$. Since $u_2 = 1$ we have $u_2|u_n$ for all positive integers n, but it is certainly not the case that $2|n$ for all positive integers n. ▲

The Corollary to Theorem 13-3 tells us that for $n > 4$ the Fibonacci number u_n is composite whenever n is composite. This follows from the fact that if $n > 4$ is composite then it may be written as a product n_1n_2 where $2 < n_1 < n$, and so $u_{n_1}|u_n$ where $1 < u_{n_1} < u_n$.

We can also use the Theorem and Corollary to prove that the multiples of a given integer n which appear in the Fibonacci sequence do so with equal spacing. For, suppose that u_m is the first Fibonacci number which is a multiple of n. Since $u_m|u_{km}$ for $k = 1, 2, \ldots$ it follows that $n|u_{km}$. Hence every mth term in the Fibonacci sequence is a multiple of n. On the other hand, these are the only multiples of n, for if $n|u_l$ then, being a common divisor of u_m and u_l, $n|\gcd(u_m, u_l)$. That is, from Theorem 13-3, $n|u_{\gcd(m,l)}$. Now as m was chosen to be the least positive integer with the property $n|u_m$ it follows that $m \leq \gcd(m, l)$. But certainly $\gcd(m, l) \leq m$ and so $\gcd(m, l) = m$. This implies that l is a positive multiple of m so that u_l is one of the u_{km}.

It might look as if this completes the proof of the result which **B** cites as cumbersome. But notice that all we have shown is that *if* a multiple of n appears in the Fibonacci sequence then infinitely many multiples of n occur with equal spacing. The proof that one multiple of n does occur will have to wait until the next unit.

SAQ 20 **B** page 293, Problems 13.1, number 8.

SAQ 21 Use the Corollary to Theorem 13-3 to

(i) find where in the Fibonacci sequence multiples of 13 occur;

(ii) show that $4|u_n$ if and only if $8|u_n$.

SAQ 22 **B** page 293, Problems 13.1, number 10.

SOLUTION TO SAQ 20 $\gcd(u_{24}, u_{36}) = u_{\gcd(24,36)} = u_{12}$, by Theorem 13-3. Therefore the common divisors of u_{24} and u_{36} are the divisors of u_{12}. By the Corollary, the Fibonacci numbers which divide u_{12} are

$$u_1 = u_2 = 1,\ u_3 = 2,\ u_4 = 3,\ u_6 = 8 \text{ and } u_{12} = 144. \quad ■$$

SOLUTION TO SAQ 21

(i) Note firstly that $u_7 = 13$. Hence, by the Corollary, $13|u_n$ if and only if $7|n$. This means that every seventh term is a multiple of 13.

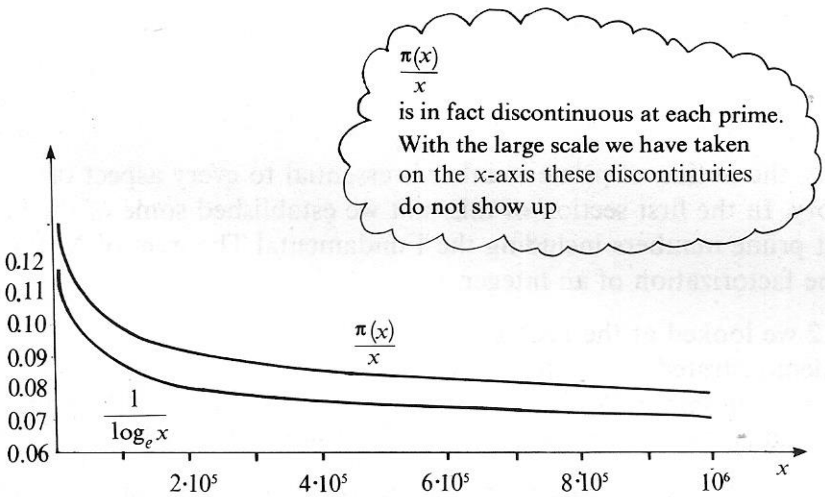
(ii) As $u_6 = 8$ we know that $8|u_n$ if and only if $6|n$, so the multiples of 8 in the Fibonacci sequence occur as every sixth term. However, we have already seen that the multiples of 4 also occur every sixth term. So every Fibonacci number which is a multiple of 4 is also a multiple of 8. ■

SOLUTION TO SAQ 22 By Theorem 13-2, $u_m|u_{mn}$ and $u_n|u_{mn}$. Furthermore, by Theorem 13-3, $\gcd(u_m, u_n) = u_{\gcd(m,n)} = u_1 = 1$. So by Corollary 2 on **B** page 28 we have $u_mu_n|u_{mn}$. ■

2.5 Epilogue

In the unit we have seen plenty of evidence for the unpredictability of occurrence of the prime numbers. On the one hand, there appear to be infinitely many pairs of successive odd integers both of which are prime (twin primes), whilst at the same time there exist arbitrarily long sequences of consecutive composite numbers. But despite this local irregularity of their distribution, when we look at the primes overall, their global distribution can be described with rather more success.

Towards the end of the eighteenth century, Gauss and Legendre observed independently that the sequence of primes 'thins out'. To be more precise, if for each positive real number x we denote by $\pi(x)$ the number of primes not exceeding x (so that, for example, $\pi(6) = 3$ and $\pi(18\frac{1}{4}) = 7$), then $\pi(x)$ is an increasing function whose rate of growth decreases as x gets large. This suggests that we might look with interest at the function $\pi(x)/x$ which measures the 'density' of the primes in the interval $(0, x]$. It turns out that $\pi(x)/x$ bears a very strong resemblance to the function $1/\log_e x$.



$\frac{\pi(x)}{x}$ **is in fact discontinuous at each prime. With the large scale we have taken on the x-axis these discontinuities do not show up**

On analysing extensive tables of primes, Gauss and Legendre observed that as x gets larger and larger the values of $\pi(x)$ seem to behave more and more like those of $x/\log_e x$. This led them to formulate a theorem which has become known as the Prime Number Theorem:

$$\lim_{x \to \infty} \left\{ \frac{\pi(x)}{x/\log_e x} \right\} = 1.$$

The effort they expended in formulating this result must have been really considerable. There were no efficient calculating devices at that time, and it is known that Gauss actually compiled by hand a table of all primes up to 3,000,000 and investigated the number of primes occurring in each group of 1000 consecutive integers.

But Gauss and Legendre were unable to prove the Prime Number Theorem. It was through the collective genius and hard work of several mathematicians in the nineteenth century—notably Dirichlet, Chebyshev, Riemann, Hadamard and de la Vallée Poussin—that the theorem was finally proved in 1896 by Hadamard, and, independently, by de la Vallée Poussin.

The proofs of the Prime Number Theorem make extensive use of complex function theory, utilizing properties of the so-called Riemann Zeta function. But in 1949, a purely arithmetic proof, not calling on techniques of complex analysis, was discovered by the Norwegian mathematician Selberg. The proof, however, is extremely complicated and beyond the scope of this, or any other first course in Number Theory.

En route to proving the Prime Number Theorem by methods of complex analysis, many other results emerge which are interesting in their own right. One merits mention here. Many beginning students of mathematics are surprised on first learning that the harmonic series

$$\sum_{n \geq 1} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n} + \cdots$$

is divergent (the sum is unbounded). If so, it must come as a shock to find that if all the terms are discarded except those where the denominator is prime then the resulting series

$$\sum_{p \,\text{prime}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

is still divergent.

For more about the history of the Prime Number Theorem, some numerical evidence for its validity, and an insight into the technical content of its proof, you might like to read the first appendix of **B**, pages 344–350.

2.6 Summary

As **B** remarks, the notion of prime number is essential to every aspect of number theory. In the first section of this unit we established some of the basic results about prime numbers including the Fundamental Theorem of Arithmetic, and the prime factorization of an integer.

In Section 2.2 we looked at the problem of investigating the primality of a given integer and demonstrated a reasonably practical method for listing all primes less than some given integer N. Showing that there exist infinitely many primes, we then obtained crude estimates of the size of the nth prime.

Section 2.3 gave some results concerning the distribution of the infinite set of primes within the set of positive integers. Included was the result that any non-constant polynomial with integer coefficients, and of an integer variable, takes on infinitely many composite values. On the other hand, Dirichlet's Theorem tells us that certain linear polynomials take on infinitely many prime values. Finally, a glance at Goldbach's Conjecture was used to illustrate the many questions which remain unanswered in this area of the subject.

Section 2.4 introduced the Fibonacci sequence and investigated divisibility properties of the Fibonacci numbers.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

UNIT 3
CONGRUENCE

3.0 Introduction

There are many occasions when properties are shared by two integers provided they differ by a multiple of some fixed integer $n \geq 2$. In the case $n = 2$, two integers differ by a multiple of 2 when they have the same parity (even or odd) and, for example, $(-1)^a = (-1)^b$ precisely when a and b have the same parity. Taking $n = 4$, it is easily derived from the Division Algorithm that two integers have the same remainder (0, 1, 2 or 3) when divided by 4 if and only if their difference is a multiple of 4. Again it is true that $\gcd(a, n) = \gcd(b, n)$ whenever $a - b$ is a multiple of n (see SAQ 4).

It is convenient to have a name and notation to describe this situation, and such is developed in the first section of this unit. Two integers a and b are said to be *congruent modulo n* provided $a - b$ is a multiple of n. This unit and the next are wholly concerned with *congruence*, a concept which will occur frequently throughout the remainder of the course.

Our first substantial application of congruence took place in the final section of *Unit 2*, although the terminology was not then at our disposal. Choosing a positive integer n, we replaced each Fibonacci number by the smallest non-negative integer to which it is congruent modulo n (its remainder on division by n), producing a new sequence which we referred to as the remainder sequence. Study of this simpler 'congruent' sequence led us to properties of the Fibonacci sequence itself.

The unit comprises Chapter 4 of **B**. Section 3.1 investigates basic properties of congruence, involving essentially re-expression of certain divisibility properties of integers. The Division Algorithm plays a crucial role in this respect. Section 3.2 turns to applications of congruence and, in particular, establishes tests for divisibility by certain integers. Section 3.3 is the core of the unit, looking at the problem of solving linear congruences (linear equations in which equality is replaced by congruence). This section culminates in a classical result concerning solutions of a system of simultaneous linear congruences, the so-called Chinese Remainder Theorem. As promised in *Unit 2*, Section 3.4 returns to our study of the Fibonacci sequence, illustrating the use of congruence in extracting properties of the sequence.

This unit again puts an emphasis on problem solving. The main objective of the unit is to enable you to solve a variety of congruence problems, in addition to appreciating how congruence problems arise naturally in mathematics. To this end, the unit contains a good number of worked examples and SAQs, and we round off with the short tape-based Section 3.5, on further problem solving.

3.1 Basic Properties of Congruence

As the title suggests, this section considers the most fundamental properties of congruence. The results obtained on the laws governing addition, multiplication and cancellation for congruences are crucial for a full understanding of the rest of the course. Fortunately, the proofs are simple and you should have no difficulty in assimilating the results immediately.

But first we learn something about the eminent mathematician Gauss, who laid the foundations of modern number theory and indeed first introduced the concept of congruence.

READ B Chapter 4, page 68, as far as page 72, line 13.

NOTE *Page 71, line 14*

Although **B**'s reference to the set of least *positive* residues modulo n is standard terminology, strictly speaking they should be called the set of least *non-negative* residues, since 0 is not positive. ▲

SAQ 1 **B** page 75, Problems 4.2, number 1.

SAQ 2 **B** page 76, Problems 4.2, number 7.

SOLUTION TO SAQ 1

(a) $a \equiv b \pmod{n}$ means that $n|a - b$. Since $m|n$ it follows (by Theorem 2-2(4), **B** page 24) that $m|a - b$. That is, $a \equiv b \pmod{m}$.

(b) As $a \equiv b \pmod{n}$ we have $a - b = kn$, for some integer k. Therefore, multiplying through by c, $ca - cb = k(cn)$, which shows that $cn|ca - cb$. That is, $ca \equiv cb \pmod{cn}$.

[Note that the condition $c > 0$ is needed because the modulus cn must be a positive integer.]

(c) From $a - b = kn$, division by d gives $\frac{a}{d} - \frac{b}{d} = k\frac{n}{d}$. As $\frac{a}{d}$, $\frac{b}{d}$ and $\frac{n}{d}$ are integers, the latter being positive, this amounts to $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. ■

SOLUTION TO SAQ 2

(a) As we are given n residues modulo n it remains to prove only that they are incongruent modulo n. Suppose therefore that

$$c + ia \equiv c + ja \pmod{n}, \text{ where } 0 \leq i, j < n.$$

This means that n divides the difference $(c + ia) - (c + ja) = (i - j)a$. But from $n|(i - j)a$ and $\gcd(a, n) = 1$, Euclid's Lemma gives us $n|(i - j)$ which in the language of congruence says $i \equiv j \pmod{n}$. The condition $0 \leq i, j < n$ now implies that $i = j$.

(b) Any set of n consecutive integers is of the form

$$c, c + 1, c + 2, \ldots, c + (n - 1)$$

and so all we need to do is observe that $\gcd(1, n) = 1$ and invoke part (a) with $a = 1$ to obtain the required result.

(c) By part (b), any set of n consecutive integers forms a complete set of residues modulo n, and so one of these integers must be congruent to 0 modulo n, i.e. it is divisible by n. As one of the integers is divisible by n so too is the product. ■

Let us glance again at some of the steps in our solution to SAQ 2(a). From the initial supposition that

$$c + ia \equiv c + ja \pmod{n},$$

the divisibility implications led us to $n|(i - j)a$, or, what is the same thing,

$$ia \equiv ja \pmod{n}.$$

So to reach this stage we have effectively subtracted c (i.e. added $-c$) to the two sides of the congruence. Next we cancelled a to reach

$$i \equiv j \pmod{n}$$

(this step being justified by Euclid's Lemma).

Notice that these are precisely the steps we would take to deduce $i = j$ if the initial congruence were replaced by ordinary equality. Indeed, there are certain similarities between the way we can manipulate congruences and the handling of corresponding equalities, which are listed in the next result, Theorem 4-2. The properties in the theorem are proved by falling back on the underlying divisibility implications, but thereafter we shall learn to manipulate congruences by using these properties without resorting to divisibility.

READ B from page 72, line 18 to page 74, line 5.

The first three parts of Theorem 4-2 establish that, for each positive integer *n*, congruence modulo *n* is an equivalence relation. Part (1) is the reflexive property, (2) the symmetric property and (3) the transitive property. For each *n* then, we have a partition of the integers into disjoint classes, two integers being in the same class if and only if they are congruent modulo *n*. These classes are called the *residue* (or congruence) *classes* modulo *n*.

In the case $n = 4$ the residue classes are

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$\{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$\{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$\{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

corresponding to the set of least positive residues $\{0, 1, 2, 3\}$. Selecting one number from each residue class, e.g. $\{-8, 5, -2, 3\}$, will always produce a complete set of residues, as we have the correct number of residues and no two of them can be congruent since they belong to different residue classes. Another choice of residues which often proves useful is the set $\{-1, 0, 1, 2\}$, where from each class we have selected a residue of least absolute size. For general $n > 1$, the set of *least absolute residues* consists of the *n* integers which satisfy the inequalities $-n/2 < x \leq n/2$. For example, $n = 7$ gives the set $\{-3, -2, -1, 0, 1, 2, 3\}$.

Part (4) of Theorem 4-2 is of great importance. In essence it says that the residue class to which a sum $a + c$ or a product ac belongs does not depend so much on the individual numbers *a* and *c* but rather on the residue classes to which they belong. Denote by $[r]$ the residue class to which *r* belongs. This will mean that residue classes are denoted in many different ways; for instance, taking $n = 5$, $[-1] = [4] = [19]$ since $-1 \equiv 4 \equiv 19 \pmod 5$. However, corresponding to the set of least positive residues, the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

is the set of all residue classes modulo *n*. Reinterpreting in terms of residue classes, (4) tells us that if $[a] = [b]$ and $[c] = [d]$, then $[a + c] = [b + \mathrm{d}]$ and $[ac] = [bd]$. This implies that the operations given by

$$[a] + [b] = [a + b]$$

and

$$[a] \times [b] = [ab]$$

are well defined (unambiguous) on $\mathbb{Z}_n$. For example, when $n = 4$ we obtain the following tables

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

where, for instance, $[3] \times [2] = [2]$ is obtained from the definition $[3] \times [2] = [3 \cdot 2] = [6]$, and the fact that $[6] = [2]$ since $6 \equiv 2 \pmod 4$.

In practice, we can reduce the amount of arithmetic in congruence problems by working with the numbers in a complete set of residues alone (the most frequent choice being the set of least positive residues although occasionally it is more appropriate to work with the least absolute residues). After each sum or product we replace the answer by the chosen residue to which it is congruent. That is, we are really using the residue class arithmetic defined above but avoiding much of the formalism. Here are a couple of illustrations.

XAMPLE 1 **B** page 76, Problems 4.2, number 6.

To verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ is a complete set of residues modulo 11 we show that, in some order, these integers are congruent modulo 11 to the members of the set of least positive residues.

$$2^2 = 4; \quad 2^3 = 8; \quad 2^4 = 16 \equiv 5; \quad 2^5 = 2 \cdot 2^4 \equiv 2 \cdot 5 \equiv 10; \quad 2^6 \equiv 2 \cdot 10 \equiv 9;$$

$$2^7 \equiv 2 \cdot 9 \equiv 7; \quad 2^8 \equiv 2 \cdot 7 \equiv 3; \quad 2^9 \equiv 2 \cdot 3 \equiv 6.$$

Together with 0, 1 and 2 these give $\{0, 1, 2, 3, 4, \ldots, 10\}$.

That $0, 1^2, 2^2, \ldots, 10^2$ is not a complete set of residues modulo 11 follows since these 11 integers are not incongruent; for instance, $1^2 \equiv 10^2 \pmod{11}$. Indeed, since $11 - r \equiv -r \pmod{11}$, Theorem 4-2(6) gives $(11 - r)^2 \equiv (-r)^2 \equiv r^2$, and taking $r = 1, 2, 3, 4$ and 5 identifies five congruent pairs amongst this set.

XAMPLE 2 Show that there do not exist integers x and y for which $x^2 + y^2 = 999$.

At first glance it is difficult to see what this question has to do with congruence. In fact, it is a particular instance of a general result concerning the possible values that the sum of two squares can take when we approach the problem working with congruence modulo 4.

Any integer x is congruent to 0, 1, 2 or 3 modulo 4. Theorem 4-2(6) tells us that x^2 is congruent to one of $0^2, 1^2, 2^2 \equiv 0$ or $3^2 \equiv 1$, modulo 4. That is, $x^2 \equiv 0$ or $1 \pmod 4$. Similarly, for any integer y, $y^2 \equiv 0$ or $1 \pmod 4$. Theorem 4-2(4) now gives $x^2 + y^2 \equiv 0, 1$ or $2 \pmod 4$ (the possible values obtained adding 0 or 1 to 0 or 1).

We conclude that no integer which is congruent to 3 modulo 4 can be expressed as the sum of two squares. But $999 \equiv 3 \pmod 4$, and so $x^2 + y^2 = 999$ has no integer solutions. ☐

There is one further result of equal importance to those of Theorem 4-2 which we include here for future reference.

HEOREM If $a \equiv b \pmod m$ and $a \equiv b \pmod n$ when $\gcd(m, n) = 1$, then $a \equiv b \pmod{mn}$.

PROOF In fact this result follows immediately from Corollary 2 on **B** page 28. From the definition of congruence we are given that $m | a - b$ and $n | a - b$. Coupled with $\gcd(m, n) = 1$, the Corollary gives $mn | a - b$. That is, $a \equiv b \pmod{mn}$. ■

Before you start work on the self-assessment questions, one word of warning. Don't fall into the trap of thinking that because $x \equiv y \pmod n$ it will follow that $a^x \equiv a^y \pmod n$. A simple counterexample is provided by the fact that $1 \equiv 4 \pmod 3$ but $2^1 \not\equiv 2^4 \pmod 3$.

SAQ 3 **B** page 76, Problems 4.2, number 4.

SAQ 4 **B** page 75, Problems 4.2, number 3.

SAQ 5 Show that if $a \equiv b \pmod m$ and $a \equiv b \pmod n$ then $a \equiv b \pmod l$, where $l = \operatorname{lcm}(m, n)$. Derive from this another proof of the Theorem preceding SAQ 3.

SAQ 6 **B** page 76, Problems 4.2, number 10, parts (a), (b), (c) and (d).

SOLUTION TO SAQ 3

(a) $2^3 = 8 \equiv 1 \pmod 7$.

Therefore $2^{48} = (2^3)^{16} \equiv 1^{16} \equiv 1 \pmod 7$

and so $2^{50} = 2^2 \cdot 2^{48} \equiv 4 \cdot 1 \equiv 4 \pmod 7$.

The remainder on dividing 2^{50} by 7 is 4.

$41 \equiv 6 \pmod 7$ (or, if you prefer, $41 \equiv -1 \pmod 7$). So $41^2 \equiv 1 \pmod 7$, and $41^{65} = 41 \cdot (41^2)^{32} \equiv 6 \cdot 1^{32} \equiv 6 \pmod 7$.

The remainder on dividing 41^{65} by 7 is 6.

(b)
$$\begin{aligned}
1 \equiv 5 \equiv 9 \equiv \cdots &\equiv 97 \pmod 4,\\
2 \equiv 6 \equiv 10 \equiv \cdots &\equiv 98 \pmod 4,\\
3 \equiv 7 \equiv 11 \equiv \cdots &\equiv 99 \pmod 4,\\
4 \equiv 8 \equiv 12 \equiv \cdots &\equiv 100 \pmod 4.
\end{aligned}$$

Therefore

$$\begin{aligned}
1^5 + 2^5 + 3^5 + \cdots + 100^5 &\equiv 25 \cdot (1^5 + 2^5 + 3^5 + 4^5) \pmod 4\\
&\equiv 25 \cdot (1^5 + 2^5 + (-1)^5 + 0) \pmod 4\\
&\equiv 25 \cdot (1 + 0 + -1 + 0) \equiv 0 \pmod 4.
\end{aligned}$$

The remainder on dividing the sum by 4 is 0. ■

SOLUTION TO SAQ 4

Since $a \equiv b \pmod n$ we have $a - b = kn$, for some integer k. Let $d_1 = \gcd(a, n)$ and $d_2 = \gcd(b, n)$. Since $d_1 | a$ and $d_1 | n$ it follows that $d_1 | a - kn$. That is, $d_1 | b$. Therefore d_1 is a common divisor of b and n, and so $d_1 \leq d_2$.

On the other hand, $d_2 | b$ and $d_2 | n$ gives $d_2 | b + kn$. That is, $d_2 | a$ and so d_2 is a common divisor of a and n, giving $d_2 \leq d_1$. Hence $d_1 = d_2$. ■

SOLUTION TO SAQ 5

Let $d = \gcd(m, n)$, so that $l = \operatorname{lcm}(m, n) = \dfrac{mn}{d}$. To show that $a \equiv b \pmod l$ we must show that there exists an integer t such that $a - b = t\left(\dfrac{mn}{d}\right)$.

Given that $a \equiv b \pmod m$ and $a \equiv b \pmod n$ we know that there exist integers r and s such that

$$a - b = rm = sn.$$

From $rm = sn$ we obtain $r\left(\dfrac{m}{d}\right) = s\left(\dfrac{n}{d}\right)$, where $\dfrac{m}{d}$ and $\dfrac{n}{d}$ are integers with $\gcd\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = 1$. It follows from Euclid's Lemma that $\dfrac{n}{d}$ divides r, and putting $r = t\left(\dfrac{n}{d}\right)$ in the above equation yields $a - b = t\left(\dfrac{mn}{d}\right)$, as required.

When $\gcd(m, n) = 1$, $\operatorname{lcm}(m, n) = mn$ and this result reduces to our earlier theorem. ■

SOLUTION TO SAQ 6

We attempted several problems of this kind in *Unit 1*, where we used the Division Algorithm. This time we are going to attack them using ideas of congruence. But notice that as the congruence properties all arise from divisibility conditions, the arguments are going to be essentially the same as those of *Unit 1*. However, we now have more succinct terminology to use and, hopefully, some improved techniques.

(a) Working with the set of least positive residues, any odd integer is congruent to one of 1, 3, 5 or 7 modulo 8. The result follows since $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \equiv 1 \pmod 8$.

(b) Working with the set of least absolute residues modulo 9, and investigating possible values of a^3:

$$0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8 \equiv -1, \quad 3^3 = 27 \equiv 0, \quad 4^3 = 64 \equiv 1,$$

$$(-4)^3 = -4^3 \equiv -1, \quad (-3)^3 = -3^3 \equiv 0, \quad (-2)^3 = -2^3 \equiv 1, \quad (-1)^3 = -1.$$

So, for any integer a, $a^3 \equiv 0, 1$ or $-1 \pmod 9$.

(c) Confirmation that, working modulo 6,

$$(-2)^3 \equiv -2, \quad (-1)^3 \equiv -1, \quad 0^3 \equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 2 \quad \text{and } 3^3 \equiv 3$$

establishes $a^3 \equiv a \pmod 6$, for all integers a.

(d) To show that $a^2 \equiv 1 \pmod{24}$ it suffices to show that $a^2 \equiv 1 \pmod 3$ and $a^2 \equiv 1 \pmod 8$, and appeal to our earlier theorem. Since we are only considering odd integers a, that $a^2 \equiv 1 \pmod 8$ has been shown in part (a).

Since $3 \nmid a$, $a \equiv 1$ or $2 \pmod 3$. So $a^2 \equiv 1^2$ or $2^2 \pmod 3$. That is, $a^2 \equiv 1 \pmod 3$, and the result follows. ■

READ B from page 74, line 6 to the end of Section 4.2.

The result of Theorem 4-3 should convince you that the utmost care is needed when you are tempted to cancel a common factor from both sides of a congruence. In fact, the theorem states that in doing so you in general produce a congruence with a *different* modulus. The two Corollaries describe situations where the modulus remains unchanged. The second Corollary, stated in terms of the arithmetic of $\mathbb{Z}_p$, where p is a prime, bears a striking resemblance to the cancellation law in the integers, since it says that if $[c][a] = [c][b]$ where $[c] \neq [0]$, then $[a] = [b]$.

SAQ 7 Use an appropriate cancellation to simplify each of the following congruences.

(a) $6x \equiv 18 \pmod{30}$

(b) $20x \equiv 30 \pmod{45}$

(c) $52x \equiv 39 \pmod{67}$

SAQ 8 **B** page 76, Problems 4.2, number 13.

SOLUTION TO SAQ 7

(a) $6x \equiv 18 \pmod{30} \implies x \equiv 3 \pmod 5$, since $\gcd(6, 30) = 6$.

(b) $20x \equiv 30 \pmod{45} \implies 2x \equiv 3 \pmod 9$. Since we are cancelling a factor 10 and $\gcd(10, 45) = 5$ we must divide the modulus by 5.

(c) $52x \equiv 39 \pmod{67} \implies 4x \equiv 3 \pmod{67}$, since $\gcd(13, 67) = 1$. ■

SOLUTION TO SAQ 8

The result in question here is a slight variation on Corollary 1. It says that we can cancel congruent numbers on either side of a congruence, provided they are relatively prime to the modulus.

Given $ab \equiv cd \pmod n$ and $b \equiv d \pmod n$, we have integers r and s such that $ab - cd = rn$ and $b - d = sn$. Using the second of these equations to eliminate d from the first produces $ab - c(b - sn) = rn$. That is, $(a - c)b = (r - sc)n$. From the fact that $\gcd(b, n) = 1$, Euclid's Lemma now gives $n \mid a - c$, which amounts to the required congruence. ■

3.2 Special Divisibility Tests

Given any integer (written in our usual decimal notation) we can tell at a glance whether it is divisible by 2 or 5 without carrying out the division. To test divisibility by 5, for example, we merely look to see whether the final digit is 0 or 5. The section introduces tests for divisibility by 3, 4, 8, 9 and 11 and shows how these tests arise out of congruence considerations.

READ B Section 4.3, page 77, as far as page 79, line 13.

NOTE *Page 77, line −4*
A somewhat shorter way of presenting the uniqueness argument is to assume that the smallest value of i for which $a_i \neq c_i$ is k, say, so that

$$a_m b^m + a_{m-1} b^{m-1} + \cdots + a_k b^k = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_k b^k.$$

Cancellation of the common factor b^k now gives

$$(a_m b^{m-k-1} + \cdots + a_{k+1})b + a_k = (c_m b^{m-k-1} + \cdots + c_{k+1})b + c_k$$

and since $0 \leq a_k, c_k < b$, the uniqueness of remainder guaranteed by the Division Algorithm gives $a_k = c_k$—a contradiction. ▲

SAQ 9 Determine the base b place value notation for 170 where (a) $b = 2$, (b) $b = 7$, (c) $b = 8$ and (d) $b = 11$.

SOLUTION TO SAQ 9 (a) Following the application of the Division Algorithm on **B** page 77,

$$\begin{aligned} 170 &= 85 \cdot 2 + 0 \\ 85 &= 42 \cdot 2 + 1 \\ 42 &= 21 \cdot 2 + 0 \\ 21 &= 10 \cdot 2 + 1 \\ 10 &= 5 \cdot 2 + 0 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

So $170 = (10101010)_2$

(b) $170 = (332)_7$.

(c) $170 = (252)_8$.

(d) $170 = (145)_{11}$. ■

READ B from page 79, line 14 to the foot of page 79.

Theorem 4-4 and its Corollary have numerous applications in finding (or more often establishing non-existence of !) integer solutions of polynomial equations. Here is an example to illustrate the general technique.

EXAMPLE 3 Show that the polynomial equation

$$P(x) = 8x^3 - 19x^2 - 9x + 6 = 0$$

has no integral solutions.

The trick for this particular equation is to consider the possible residues of $P(x)$ modulo 5. By the theorem, it suffices to let x take all values in a complete set of residues modulo 5, say $\{0, 1, 2, 3, 4\}$, for if x is any integer than it is congruent to one of these five residues, and consequently $P(x)$ is congruent modulo 5 to one of $P(0)$, $P(1)$, $P(2)$, $P(3)$ or $P(4)$. To determine these values we can first simplify the polynomial $P(x)$ by reducing its coefficients modulo 5:

$$P(x) \equiv 3x^3 + x^2 + x + 1 \pmod{5}.$$

Then

x	0	1	2	3	4
$P(x) \pmod{5}$	1	1	1	4	3

shows that the congruence $P(x) \equiv 0 \pmod{5}$ has *no* solutions. It now follows that $P(x) = 0$ cannot have any integral solutions, because if x_0 is an integer such that $P(x_0) = 0$, then $P(x_0) \equiv 0 \pmod{n}$ for every positive integer n, contradicting what we have shown to be the case for $n = 5$.

Note that the above argument would have failed if instead we had worked modulo 2, modulo 3 or modulo 4, for we would have found that $P(0) \equiv 0 \pmod{2}$, $P(0) \equiv 0 \pmod{3}$ and $P(2) \equiv 0 \pmod{4}$, despite $P(x) = 0$ having no integral solution. In other words, *no* solution to a corresponding congruence guarantees *no* solution to the original equation, but a solution to the congruence does not settle the equation question either way.

SAQ 10 Show that the following equations have no integral solutions.

(a) $x^4 + x^3 + x^2 + x + 1 = 0$

(b) $3x^4 - 4x^3 + 13x^2 - 5x + 4 = 0.$

SOLUTION TO SAQ 10 For both parts we adopt the method of Example 3. To show that the equation $P(x) = 0$ has no integral solutions it is sufficient to find a positive integer n such that the corresponding congruence $P(x) \equiv 0 \pmod{n}$ has no solutions.

(a) Let $P(x) = x^4 + x^3 + x^2 + x + 1$ and consider the congruence $P(x) \equiv 0 \pmod{2}$. Taking $\{0, 1\}$ as complete set of residues modulo 2, $P(0) \equiv 1 \pmod{2}$ and $P(1) \equiv 1 \pmod{2}$ confirms that the congruence has no solutions.

(b) Let $P(x) = 3x^4 - 4x^3 + 13x^2 - 5x + 4$. Since $P(0) = 4$, we see that the congruence $P(x) \equiv 0 \pmod{2}$ has a solution, and so working modulo 2 will not help us. Try modulo 3. First simplifying the coefficients modulo 3, we hope to find that the congruence

$$P(x) \equiv 2x^3 + x^2 + x + 1 \equiv 0 \pmod{3}$$

has no solutions. Substituting $x = 0$, 1 and 2 we obtain $P(0) \equiv 1 \pmod{3}$, $P(1) \equiv 2 \pmod{3}$ and $P(2) \equiv 2 \pmod{3}$, confirming that the congruence indeed has no solutions. ■

READ B from the top of page 80 to the end of Section 4.3.

SAQ 11 **B** page 81, Problems 4.3, number 5.

SAQ 12 **B** page 81, Problems 4.3, number 6, with the additional part:
(e) Find a test for divisibility by 8.

SAQ 13 **B** page 81, Problems 4.3, number 10, part (a).

SOLUTION TO SAQ 11

(a) The 9-test won't help here as it fails to distinguish between the digits 0 and 9. Using the 11-test:

$$52817 \equiv 7 - 1 + 8 - 2 + 5 = 17 \equiv 6 \pmod{11},$$

$$3212146 \equiv 6 - 4 + 1 - 2 + 1 - 2 + 3 \equiv 3 \pmod{11},$$

and so $52817 \cdot 3212146 \equiv 6 \cdot 3 \equiv 7 \pmod{11}$.

Now $$\begin{aligned} 169655x15282 &\equiv 2 - 8 + 2 - 5 + 1 - x + 5 - 5 + 6 - 9 + 6 - 1 \\ &\equiv 5 - x \pmod{11}. \end{aligned}$$

Hence $5 - x \equiv 7 \pmod{11}$ (and $0 \le x \le 9$) gives $x = 9$.

(b) $[3(523 + x)]^2 = 9(523 + x)^2 \equiv 0 \pmod 9$.

Using the 9-test:

$$2x99561 \equiv 2 + x + 9 + 9 + 5 + 6 + 1 \equiv 32 + x \equiv 5 + x \pmod 9.$$

So we require $5 + x \equiv 0 \pmod 9$, which gives $x = 4$ as the only possibility. ■

SOLUTION TO SAQ 12

Throughout this solution we let $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ where $0 \le a_i \le 9$ for each i.

(a) Since $10 \equiv 0 \pmod 2$, $N \equiv a_0 \pmod 2$ and N is divisible by 2 (i.e. is congruent to 0 modulo 2) if and only if a_0 is divisible by 2. This occurs when $a_0 = 0, 2, 4, 6$ or 8.

(b) Since $10 \equiv 1 \pmod 3$, $10^k \equiv 1 \pmod 3$ for all $k \ge 1$ and so $N \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \pmod 3$. The result follows.

(c) As $10^k \equiv 0 \pmod 4$ for all $k \ge 2$ we have that $N \equiv a_1 10 + a_0 \pmod 4$ which gives the required result.

(d) As $10 \equiv 0 \pmod 5$, $N \equiv a_0 \pmod 5$ showing that N is divisible by 5 precisely when $a_0 = 0$ or 5.

(e) Extending the idea of part (c) gives us a test for divisibility by 8. Since $8 \mid 1000$ it follows that $10^k \equiv 0 \pmod 8$ for all $k \ge 3$. Therefore $N \equiv a_2 10^2 + a_1 10 + a_0 \pmod 8$. This means that N is divisible by 8 if and only if the integer formed by taking the final three digits of N is itself divisible by 8. ■

SOLUTION TO SAQ 13

Since N and M are made up of the same digits (albeit in different orders), the sum of the digits in N is equal to the sum of the digits in M. By the 9-test, $N \equiv M \pmod 9$ and so $9 \mid N - M$. ■

3.3 Linear Congruences

In the previous section we introduced the idea of solving congruences $P(x) \equiv 0 \pmod n$, where P is a polynomial with integer coefficients. In the particular case when P has degree 1 we have a *linear congruence*. The next reading passage is concerned with the solutions of linear congruences.

As we shall see, there is a very strong relationship between linear congruences and linear Diophantine equations; indeed, our work on the latter (Section 1.7 of *Unit 1*) leads us to a result on the solvability (and number of solutions) of the general linear congruence. In practice, however, we shall acquire techniques for solving linear congruences without resorting to the method of *Unit 1* (where we employed the Euclidean Algorithm).

READ B Section 4.4 from page 82 as far as page 85, line -6.

NOTES (i) *Page 83, line 12*

The proof of Theorem 4-7 may, at first glance, look long and involved, but in reality there is very little to it. Observing that the solutions of $ax \equiv b \pmod{n}$ are precisely the x-values in solutions of the linear Diophantine equation $ax - ny = b$, Theorem 2-9 (on **B** page 40) has already done the bulk of the work. That theorem tells us that the linear congruence has solutions if and only if d divides b, where $d = \gcd(a, n)$ and if x_0 is one solution then the others are the values of $x_0 - \frac{nt}{d}$, as t runs through all integers. All that remains here is to determine how many of these solutions are different, that is, how many are incongruent modulo n. The claim made is that if $x = x_0$ is one solution then

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \ldots,\ x_0 + (d-1)\frac{n}{d}$$

is a 'complete' set of d incongruent solutions modulo n. To justify this we must show that (i) no two members of this set are congruent modulo n, and (ii) that any solution, i.e. $x_0 - \frac{n}{d}t$ for any integer t, is congruent modulo n to one of the members of this set. (i) follows immediately when we observe that the maximum difference between members of the set is $(d-1)\frac{n}{d}$ which is less than n, so the difference between distinct members of the set cannot possibly be divisible by n. As for (ii), let t be any integer and note that $t \equiv r \pmod{d}$ for some r belonging to $\{0, 1, 2, \ldots, d-1\}$, which is a complete set of residues modulo d. Then by SAQ 1, $t\frac{n}{d} \equiv r\frac{n}{d} \pmod{n}$ and, by Theorem 4-2(4), $x_0 + \frac{n}{d}t \equiv x_0 + \frac{r}{d}t \pmod{n}$ as required.

(ii) *Page 85, line 19*

If you do not follow the sentence in brackets explaining the simplification, do not worry about it at this stage. We shall expand this point and look for other such simplifications in SAQ 15.

(iii) *Page 85, line -6*

In Example 4-7, the linear congruence $9x \equiv 21 \pmod{30}$ is said by **B** to be 'equivalent' to the linear congruence $3x \equiv 7 \pmod{10}$. This is justified by the fact that the two congruences have the same solution set: an integer x is a solution of one of the congruences if and only if it is also a solution of the other. And yet there appears to be a distinction when, having found $x \equiv 9 \pmod{10}$ to be the *unique* solution of $3x \equiv 7 \pmod{10}$, we find that the congruence $9x \equiv 21 \pmod{30}$ has *three* incongruent solutions modulo 30. But these two solutions sets are the same; the set of integers which are congruent modulo 30 to either 9, 19 or 29 is precisely the residue class of 9 modulo 10. The only difference is in the choice of expressing the solution in terms of modulo 10 or 30. ▲

A natural question here is to ask why we should want to express the solution in terms of modulo 30 when we have a more compact solution in terms of modulo 10. Indeed, given a linear congruence $ax \equiv b \pmod{n}$ in which $d|b$, where $d = \gcd(a, n)$, why do we not always start by dividing through by common factor d and look instead for the unique solution of $\frac{a}{d}x \equiv \frac{b}{d}\left(\bmod \frac{n}{d}\right)$, so that the real result we need is not Theorem 4-7 but rather its simpler Corollary? The answer lies in the nature of the problem in which the linear congruence to be solved has arisen. If we are asked to solve, in isolation, the linear congruence $ax \equiv b \pmod{n}$, then the best approach is to remove all common factors of a, b and n and aim for the unique solution (if there is one) in terms of the reduced modulus. In practice, however, if the linear congruence arises at some stage of a problem, frequently it will be necessary to solve the congruence in terms of the original modulus n. To do this we can either find one solution and then appeal to Theorem 4-7 (as **B** did in Example 4-6), or we can remove common factors, find the unique solution in terms of the reduced modulus, and then re-express the solution in terms of the original modulus (as **B** did in Example 4-7).

SAQ 14 Use Theorem 4-7 to solve the linear congruences

(a) $8x \equiv 34 \pmod{60}$,

(b) $4x \equiv 13 \pmod{47}$,

(c) $6x \equiv 15 \pmod{33}$,

(d) $95x + 20 \equiv 0 \pmod{55}$.

SAQ 15 (a) If $\gcd(a, n) = 1$, prove that $\{0, a, 2a, \ldots, (n-1)a\}$ is a complete set of residues modulo n. Deduce that there exists an integer c such that $ca \equiv 1 \pmod{n}$.

(b) If $\gcd(c, n) = 1$, prove that the congruences $ax \equiv b \pmod{n}$ and $cax \equiv cb \pmod{n}$ are equivalent. Hence,

(c) solve the following linear congruences:

(i) $5x \equiv 11 \pmod{19}$,

(ii) $3x \equiv 19 \pmod{29}$,

(iii) $17x \equiv 6 \pmod{49}$,

(iv) $11x \equiv 4 \pmod{75}$.

(d) What is wrong with the following argument?

To solve $7x \equiv 1 \pmod{40}$.

Multiplying though by 6 gives

$$42x \equiv 6 \pmod{40}.$$

That is,

$$2x \equiv 6 \pmod{40},$$

or

$$x \equiv 3 \pmod{40}.$$

[Note that $7 \cdot 3 \not\equiv 1 \pmod{40}$, so something has gone wrong!]

SAQ 16 **B** page 89, Problems 4.4, number 2.

SOLUTION TO SAQ 14

(a) Since $\gcd(8, 60) = 4$ and $4 \nmid 34$ this congruence has no solutions.

(b) Since $\gcd(4, 47) = 1$ this congruence has a unique solution modulo 47. Observing that $13 \equiv 60 \pmod{47}$, the congruence can be written as $4x \equiv 60 \pmod{47}$ from which we 'spot' the solution $x \equiv 15 \pmod{47}$.

COMMENT If you failed to spot this solution you could have found it by resorting to the method of Section 1.7, using the Euclidean Algorithm to solve the linear Diophantine equation $4x + 47y = 13$. As a general rule, however, you should be able to avoid falling back on this method. SAQ 15 outlines a much improved method, and in Section 3.5 we discuss a systematic approach to solving linear congruences where the overall strategy is to keep simplifying the congruence until such time as a solution can be spotted.

(c) $\gcd(6, 33) = 3$ and $3|15$ so the congruence has *three* solutions modulo 33. As $15 \equiv 48 \pmod{33}$, we spot that $x \equiv 8 \pmod{33}$ is one solution. By Theorem 4-7 the others are $x \equiv 8 + \frac{33}{3} \equiv 19 \pmod{33}$ and $x \equiv 8 + 2 \cdot \frac{33}{3} \equiv 30 \pmod{33}$.

(d) Since $95 \equiv 40 \pmod{55}$ and $-20 \equiv 35 \pmod{55}$ we first rewrite the congruence as $40x \equiv 35 \pmod{55}$. Now $\gcd(40, 55) = 5$ and $5|35$ so the congruence has five solutions modulo 55. One of them is seen to be $x \equiv 5 \pmod{55}$ and so by Theorem 4-7 the complete solution is $x \equiv 5, 16, 27, 38, 49 \pmod{55}$. ■

SOLUTION TO SAQ 15

(a) As the given set contains n residues we need show only that no two of them are congruent modulo n. This follows immediately, for if $ra \equiv sa \pmod{n}$, the given condition $\gcd(a, n) = 1$ permits us to cancel a, obtaining $r \equiv s \pmod{n}$. But $\{0, 1, 2, \ldots, n-1\}$ is a complete set of residues modulo n and so no two can be congruent.

Since $\{0, a, 2a, \ldots, (n-1)a\}$ is a complete set of residues, one of the members, say ca, is congruent to 1 modulo n.

(b) If $ax \equiv b \pmod{n}$ then certainly $cax \equiv cb \pmod{n}$, since $n|ax - b$ implies $n|c(ax - b)$.

On the other hand, if $cax \equiv cb \pmod{n}$ where $\gcd(c, n) = 1$, then cancellation yields $ax \equiv b \pmod{n}$.

(c) All the congruences have a unique solution to the given modulus.

(i) Multiply through by 4:

$$20x \equiv 44 \pmod{19} \iff x \equiv 6 \pmod{19}.$$

(ii) Multiply through by 10:

$$30x \equiv 190 \pmod{29} \iff x \equiv 16 \pmod{29}.$$

In each of the two remaining congruences it is not easy to spot which integer to multiply by so as to reduce the coefficient of x to 1, although the existence of such an integer is ensured by part (a). Undaunted, we can still use part (b) to simplify the congruence.

(iii) Multiply through by 3:

$$51x \equiv 18 \pmod{49} \iff 2x \equiv 18 \pmod{49}.$$

The solution $x \equiv 9 \pmod{49}$ is now apparent.

(iv) Multiply through by 7:

$$77x \equiv 28 \pmod{75} \iff 2x \equiv 28 \pmod{75}.$$

This has solution $x \equiv 14 \pmod{75}$.

(d) There are *two* errors in the argument. To start with, look at the final step. From $2x \equiv 6 \pmod{40}$ we attempted to deduce that $x \equiv 3 \pmod{40}$. But $\gcd(2, 40) = 2$ and so the former congruence has two solutions modulo 40. If we wish to cancel the common factor 2 then the correct deduction is that $x \equiv 3 \pmod{20}$ which gives the two solutions $x \equiv 3, 23 \pmod{40}$. (Notice that $x \equiv 23 \pmod{40}$ is the correct solution of the original congruence.) This explains why the argument failed to produce the correct answer, but still does not account for the presence of the erroneous solutions.

The initial error is in the first step where we multiplied through by 6. Since $\gcd(6, 40) \neq 1$ we cannot do this! Notice the resulting congruence $42x \equiv 6 \pmod{40}$ has $\gcd(40, 42) = 2$ incongruent solutions modulo 40, whereas the congruence to be solved has a unique solution modulo 40. ■

SOLUTION TO SAQ 16

(a) Any solution of $4x + 51y = 9$ requires $4x \equiv 9 \pmod{51}$ and $51y \equiv 9 \pmod 4$, so we first solve these congruences.

$$4x \equiv 9 \pmod{51} \iff 13 \cdot 4x \equiv 13 \cdot 9 \pmod{51} \iff x \equiv 15 \pmod{51}$$

$$51y \equiv 9 \pmod 4 \iff 3y \equiv 1 \pmod 4 \iff y \equiv 3 \pmod 4$$

So in any solution, x is of the form $15 + 51t$ and y of the form $3 + 4s$ and to find which values of s and t produce solutions we substitute back into the original equation:

$$4(15 + 51t) + 51(3 + 4s) = 213 + 204s + 204t = 9$$

which gives $s + t = -1$.

The solution set is therefore

$$\{x = 15 + 51t, \quad y = -1 - 4t\text{: for any integer } t\}.$$

(b) $$12x \equiv 331 \pmod{25} \iff 12x \equiv 6 \pmod{25}$$
$$\iff 24x \equiv 12 \pmod{25} \iff x \equiv -12 \equiv 13 \pmod{25}$$

$$25y \equiv 331 \pmod{12} \iff y \equiv 7 \pmod{12}$$

So $x = 13 + 25t$, $y = 7 + 12s$ and

$$12(13 + 25t) + 25(7 + 12s) = 331 + 300t + 300s = 331,$$

giving $s + t = 0$. So the solution set is

$$\{x = 13 + 25t, \quad y = 7 - 12t\text{: for any integer } t\}.$$

(c) $$5x \equiv 17 \pmod{53} \iff 5x \equiv 70 \pmod{53} \iff x \equiv 14 \pmod{53}$$

$$53y \equiv -17 \pmod 5 \iff 3y \equiv 3 \pmod 5 \iff y \equiv 1 \pmod 5$$

So $x = 14 + 53t$, $y = 1 + 5s$ and

$$5(14 + 53t) - 53(1 + 5s) = 17 + 265t - 265s = 17,$$

so that $s = t$. The solution set is therefore

$$\{x = 14 + 53t, \quad y = 1 + 5t\text{: for any integer } t\}. \quad \blacksquare$$

READ B from page 86, line 14 to page 88, line -12.

NOTE *Page 87, line 12*

The Chinese Remainder Theorem is proved by actually constructing a simultaneous solution. This is the integer $\bar{x}$ appearing in the tenth line of **B**'s proof. There are, however, a large number of variables involved and it might be helpful to read the numerical Example 4-8 on page 88 at the same time, to help keep track of what is what as you read the proof. ▲

SAQ 17 **B** page 89, Problems 4.4, number 4, parts (c) and (d).

SOLUTION TO SAQ 17

(c) To follow the steps of the Chinese Remainder Theorem we first note that

$$a_1 = 5, \quad a_2 = 4, \quad a_3 = 3, \quad n_1 = 6, \quad n_2 = 11, \quad \text{and } n_3 = 17.$$

Then $n = n_1 n_2 n_3 = 1122$, $N_1 = n_2 n_3 = 187$, $N_2 = n_1 n_3 = 102$ and $N_3 = n_1 n_2 = 66$. We next solve the congruences $N_i x \equiv 1 \pmod{n_i}$.

$$N_1 x = 187x \equiv 1 \pmod 6 \iff x \equiv 1 \pmod 6\text{, so } x_1 \equiv 1 \pmod 6$$

$$N_2 x = 102x \equiv 1 \pmod{11} \iff 3x \equiv 1 \pmod{11}$$
has solution $x_2 \equiv 4 \pmod{11}$

$$N_3 x = 66x \equiv 1 \pmod{17} \iff 15x \equiv 1 \pmod{17}$$
has solution $x_3 \equiv 8 \pmod{17}$

Now

$$\bar{x} = 5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot 4 + 3 \cdot 66 \cdot 8 = 4151$$

and so the unique solution of the system is

$$\bar{x} \equiv 4151 \equiv 785 \pmod{1122}.$$

(d) There is an initial stage to this problem in that we must first express each of the congruences in the form $x \equiv a_i \pmod{n_i}$.

$$\begin{aligned}
2x &\equiv 1 \pmod{5} &\iff\quad x &\equiv 3 \pmod{5}\\
3x &\equiv 9 \equiv 3 \pmod{6} &\iff\quad x &\equiv 1 \pmod{2}\\
4x &\equiv 1 \pmod{7} &\iff\quad x &\equiv 2 \pmod{7}\\
5x &\equiv 9 \pmod{11} &\iff\quad x &\equiv 4 \pmod{11}
\end{aligned}$$

To solve the system using the Chinese Remainder Theorem is now just (careful) arithmetic. The variable values are

$$a_1 = 3, \quad a_2 = 1, \quad a_3 = 2, \quad a_4 = 4$$

$$n_1 = 5, \quad n_2 = 2, \quad n_3 = 7, \quad n_4 = 11$$

$$n = 770, \quad N_1 = 154, \quad N_2 = 385, \quad N_3 = 110, \quad N_4 = 70$$

$$x_1 \equiv 4 \pmod{5}, \quad x_2 \equiv 1 \pmod{2}, \quad x_3 \equiv 3 \pmod{7}, \quad x_4 \equiv 3 \pmod{11}$$

and finally

$$\bar{x} \equiv 3733 \equiv 653 \pmod{770}. \quad \blacksquare$$

The two examples in SAQ 17 illustrate a drawback in using the method suggested by the proof of the Chinese Remainder Theorem to solve simultaneous linear congruences, namely that the amount of arithmetic involved can become tedious. There is an alternative method.

Suppose that a system of simultaneous linear congruences fulfils the conditions of the Chinese Remainder Theorem. Then we are assured of a unique solution modulo *n*, where *n* is the least common multiple of the moduli in the system. A simple-minded approach would be to find all incongruent solutions modulo *n* of each congruence individually and then pick out the unique common one. How we might do this in practice is illustrated by the following.

EXAMPLE 4 Solve the simultaneous congruences

$$x \equiv 9 \pmod{13}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 1 \pmod{3}.$$

$$\begin{array}{lll}
x \equiv 9 \pmod{13} \implies & x = 9, 22, 35, 48, \ldots & \text{(Increase by 13 until we}\\
& \quad\quad\quad\quad\quad\quad\downarrow & \text{reach a solution of the}\\
\quad\text{and} & & \text{second congruence)}\\
x \equiv 3 \pmod{5} \implies & \quad\quad\quad x = 48, 113, 178, \ldots & \text{(Increase by } 5 \cdot 13 \text{ until}\\
& & \text{we reach a solution of the}\\
\quad\text{and} & \quad\quad\quad\quad\quad\quad\quad\quad\quad\downarrow & \text{third congruence)}\\
x \equiv 1 \pmod{3} \implies & \quad\quad\quad x \equiv 178 \pmod{3 \cdot 5 \cdot 13} &
\end{array}$$

The Chinese Remainder Theorem tells us that the first two congruences have a unique simultaneous solution modulo $5 \cdot 13$, which we find to be 48. Amongst those integers in the residue class of 48 modulo 65 we seek the least positive member which is congruent to 1 modulo 3.

In Example 4-9, **B** uses this method, only he backs up his working with algebraic reasoning.

READ B Example 4-9 on pages 88 and 89.

This example illustrates one situation in which simultaneous linear congruences arise naturally. If n has canonical prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then solving the linear congruence $ax \equiv b \pmod{n}$ is equivalent to solving the simultaneous system

$$ax \equiv b \pmod{p_1^{k_1}}, \dots, ax \equiv b \pmod{p_r^{k_r}}.$$

The equivalence follows from our Theorem on page 47 which tells us that any simultaneous solution of the system must be a solution of the original congruence. On the other hand, any solution of $ax \equiv b \pmod{n}$ certainly satisfies $ax \equiv b \pmod{p_i^{k_i}}$, since $p_i^{k_i} | n$, for $1 \le i \le r$.

SAQ 18 **B** page 89, Problems 4.4, number 5.

SAQ 19 **B** page 90, Problems 4.4, number 10.

SOLUTION TO SAQ 18 We first solve the individual congruences.

$$\begin{array}{lclcl}
17x \equiv 3 \pmod{2} & \Leftrightarrow & x \equiv 1 \pmod{2} & & \\
17x \equiv 3 \pmod{3} & \Leftrightarrow & 2x \equiv 0 \pmod{3} & \Leftrightarrow & x \equiv 0 \pmod{3} \\
17x \equiv 3 \pmod{5} & \Leftrightarrow & 2x \equiv 3 \pmod{5} & \Leftrightarrow & x \equiv 4 \pmod{5} \\
17x \equiv 3 \pmod{7} & \Leftrightarrow & 3x \equiv 3 \pmod{7} & \Leftrightarrow & x \equiv 1 \pmod{7}
\end{array}$$

$$\begin{array}{lcll}
x \equiv 1 \pmod{2} & \Longrightarrow & x = 1, 3, \dots & \text{(Increase by 2 until we reach } x \equiv 0 \text{ (mod 3))} \\
\text{and} & & \downarrow & \\
x \equiv 0 \pmod{3} & \Longrightarrow & x = 3, 9, \dots & \text{(Increase by } 2 \cdot 3 \text{ until we reach } x \equiv 4 \text{ (mod 5))} \\
\text{and} & & \downarrow & \\
x \equiv 4 \pmod{5} & \Longrightarrow & x = 9, 39, 69, 99, \dots & \text{(Increase by 30 until we reach } x \equiv 1 \text{ (mod 7))} \\
\text{and} & & \downarrow & \\
x \equiv 1 \pmod{7} & \Longrightarrow & x \equiv 99 \pmod{210} & \blacksquare
\end{array}$$

SOLUTION TO SAQ 19 Let x be the number of gold coins. The given facts translate into the congruences

$$x \equiv 3 \pmod{17}, \quad x \equiv 10 \pmod{16}, \quad x \equiv 0 \pmod{15}$$

and our task is to find the least positive simultaneous solution.

This time we use the algebraic method of Example 4-9. From the third congruence we have $x = 15k$, for some integer k. Substituting into the second congruence we have $15k \equiv 10 \pmod{16}$, or $3k \equiv 2 \pmod{16}$, which solves to give $k \equiv 6 \pmod{16}$. Writing $k = 16l + 6$ we now have $x = 15(16l + 6) = 240l + 90$, and any number of this form satisfies the second and third congruences. Finally, we substitute into the first congruence:

$$240l + 90 \equiv 3 \pmod{17} \Leftrightarrow 2l + 5 \equiv 3 \pmod{17}$$

which gives $l \equiv 16 \pmod{17}$. So writing $l = 17m + 16$, we have

$$x = 240(17m + 16) + 90 = 4080m + 3930$$

so that the solution of the system is $x \equiv 3930 \pmod{4080}$, and the number of gold coins is 3930. $\blacksquare$

3.4 The Fibonacci Sequence Revisited

In the final section of *Unit 2* we studied **B** Section 13.1, which was concerned with the Fibonacci sequence and some of its properties. Amongst other things, we proved the following theorem for the particular cases $m = 3, 4, 5$ and 6.

THEOREM For any integer $m \geq 1$ there exist infinitely many Fibonacci numbers which are multiples of m; these multiples occur with equal spacing in the Fibonacci sequence.

The Corollary on **B** page 292 went some way towards proving this Theorem, as it showed that if *one* multiple of m occurs in the Fibonacci sequence then infinitely many do, with equal spacing. To complete the proof it remains to show only that one multiple of each integer $m \geq 1$ occurs as a Fibonacci number. This is the goal of the section, but to achieve it we first consider a different approach to the Fibonacci sequence which, as a by-product, discovers new proofs of the divisibility properties and new identities between Fibonacci numbers. Everything hinges on the following result:

THEOREM Let $\mathbf{A}$ be the matrix $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Then for all integers $n \geq 1$,

$\mathbf{A}^n = \begin{pmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{pmatrix}$, where u_n are the Fibonacci numbers, and $u_0 = 0$.

PROOF (by Mathematical Induction)

Since $u_0 = 0$ and $u_1 = u_2 = 1$, the result is certainly true when $n = 1$.

Suppose that $\mathbf{A}^k = \begin{pmatrix} u_{k-1} & u_k \\ u_k & u_{k+1} \end{pmatrix}$ for some integer $k \geq 1$. Then,

$$\mathbf{A}^{k+1} = \mathbf{A}\mathbf{A}^k = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} u_{k-1} & u_k \\ u_k & u_{k+1} \end{pmatrix}$$

$$= \begin{pmatrix} u_k & u_{k+1} \\ u_{k-1} + u_k & u_k + u_{k+1} \end{pmatrix} = \begin{pmatrix} u_k & u_{k+1} \\ u_{k+1} & u_{k+2} \end{pmatrix}$$

which is of the required form. The result follows by the First Principle of Finite Induction. ■

This apparently simple result is in fact rather powerful and leads to simple proofs of Fibonacci identities. For example, since $\mathbf{A}^{2n} = (\mathbf{A}^n)^2$ we have that

$$\begin{pmatrix} u_{2n-1} & u_{2n} \\ u_{2n} & u_{2n+1} \end{pmatrix} = \begin{pmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{pmatrix}^2 = \begin{pmatrix} u_{n-1}^2 + u_n^2 & u_{n-1}u_n + u_nu_{n+1} \\ u_{n-1}u_n + u_nu_{n+1} & u_n^2 + u_{n+1}^2 \end{pmatrix}.$$

So $u_{2n-1} = u_{n-1}^2 + u_n^2$ and $u_{2n} = u_{n-1}u_n + u_nu_{n+1}$, for all integers $n \geq 1$.

Similarly, from the matrix identity $\mathbf{A}^{m+n} = \mathbf{A}^m \cdot \mathbf{A}^n$, equating elements in the first row and second column gives the identity $u_{m+n} = u_{m-1}u_n + u_mu_{n+1}$, whose inductive proof on **B** pages 289 and 290 was far from straightforward.

Notice that the matrix $\mathbf{A}$ has multiplicative inverse $\mathbf{A}^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$. (You can check that $\mathbf{A}\mathbf{A}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$, the identity matrix.) It follows that for each integer $n \geq 1$ the matrix $\mathbf{A}^n$ has an inverse, namely $(\mathbf{A}^{-1})^n$. As is usual when dealing with exponents we abbreviate $(\mathbf{A}^{-1})^n$ by $\mathbf{A}^{-n}$, and take $\mathbf{A}^0$ to be $\mathbf{I}$. (The set of all powers of $\mathbf{A}$, $\{\mathbf{A}^n : n \in \mathbb{Z}\}$, is an infinite cyclic group in which the usual laws for exponents hold.)

In the SAQ that follows we obtain an explicit formulation for $\mathbf{A}^{-n}$ in terms of Fibonacci numbers, and use the result to obtain more Fibonacci identities.

SAQ 20 (a) Prove, using Mathematical Induction, that $\mathbf{A}^{-n} = (-1)^n \begin{pmatrix} u_{n+1} & -u_n \\ -u_n & u_{n-1} \end{pmatrix}$, for all integers $n \geq 1$.

(b) From (a), deduce the identity $u_n^2 - u_{n-1}u_{n+1} = (-1)^{n-1}$, for $n \geq 1$.

(c) Prove that $\mathbf{A}^n + (-1)^n \mathbf{A}^{-n} = (u_{n+1} + u_{n-1})\mathbf{I}$, for $n \geq 1$.

(d) By multiplying both sides of the equation in (c) by $\mathbf{A}^m$, show that

$$u_{m+n} + (-1)^n u_{m-n} = (u_{n+1} + u_{n-1}) u_m$$

for all positive integers m and n with $m \geq n$.

SOLUTION TO SAQ 20 (a) $\mathbf{A}^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} = (-1)^1 \begin{pmatrix} u_2 & -u_1 \\ -u_1 & u_0 \end{pmatrix}$, so the result is true when $n = 1$.

Assume that the result is true for some integer $k \geq 1$, i.e.

$$\mathbf{A}^{-k} = (\mathbf{A}^{-1})^k = (-1)^k \begin{pmatrix} u_{k+1} & -u_k \\ -u_k & u_{k-1} \end{pmatrix}.$$

Now

$$\begin{aligned} \mathbf{A}^{-(k+1)} = \mathbf{A}^{-k}\mathbf{A}^{-1} &= (-1)^k \begin{pmatrix} u_{k+1} & -u_k \\ -u_k & u_{k-1} \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= (-1)^k \begin{pmatrix} -(u_{k+1} + u_k) & u_{k+1} \\ u_k + u_{k-1} & -u_k \end{pmatrix} \\ &= (-1)^{k+1} \begin{pmatrix} u_{k+2} & -u_{k+1} \\ -u_{k+1} & u_k \end{pmatrix} \end{aligned}$$

which is in the required form, completing the proof.

(b)

$$\begin{aligned} \mathbf{A}^{-n} \cdot \mathbf{A}^n &= (-1)^n \begin{pmatrix} u_{n+1} & -u_n \\ -u_n & u_{n-1} \end{pmatrix} \begin{pmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{pmatrix} \\ &= (-1)^n \begin{pmatrix} u_{n+1}u_{n-1} - u_n^2 & 0 \\ 0 & u_{n+1}u_{n-1} - u_n^2 \end{pmatrix} \end{aligned}$$

But $\mathbf{A}^{-n} \cdot \mathbf{A}^n = \mathbf{I}$ and so $(-1)^n(u_{n+1}u_{n-1} - u_n^2) = 1$, which amounts to the required identity.

[To prove this identity by traditional methods is quite involved; see **B** page 294.]

(c)

$$\begin{aligned} \mathbf{A}^n + (-1)^n \mathbf{A}^{-n} &= \begin{pmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{pmatrix} + (-1)^n(-1)^n \begin{pmatrix} u_{n+1} & -u_n \\ -u_n & u_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} u_{n-1} + u_{n+1} & 0 \\ 0 & u_{n-1} + u_{n+1} \end{pmatrix} \\ &= (u_{n-1} + u_{n+1})\mathbf{I}. \end{aligned}$$

(d) Multiplying through the equation in (c) by $\mathbf{A}^m$ produces

$$\mathbf{A}^{m+n} + (-1)^n \mathbf{A}^{m-n} = (u_{n+1} + u_{n-1})\mathbf{A}^m.$$

Now equating the elements in the first row and second column of the matrices on either side of the equation gives the required formula. ■

For each integer n, positive or negative, we have seen that the entries in the matrix $\mathbf{A}^n$ are all integers, so that in this work so far we have dealt exclusively with the set of 2×2 matrices whose entries are in $\mathbb{Z}$, which we denote by $M(\mathbb{Z})$. At this point we are going to bring congruence into play. Choosing an integer

$m > 1$, we switch tack by considering matrices in $M(\mathbb{Z}_m)$, the set of 2×2 matrices whose entries are residue classes modulo m. With each matrix in $M(\mathbb{Z})$ we associate, in a natural way, a matrix in $M(\mathbb{Z}_m)$ by replacing each entry by its congruence class modulo m. For example if $m = 4$, then the matrix associated with $\begin{pmatrix} 5 & -1 \\ 4 & 6 \end{pmatrix}$ is $\begin{pmatrix} [5] & [-1] \\ [4] & [6] \end{pmatrix} = \begin{pmatrix} [1] & [3] \\ [0] & [2] \end{pmatrix}$. It seems natural to use the notation $[\mathbf{A}]$ for the matrix associated through congruence modulo m with $\mathbf{A}$. (If you have a phobia for the square bracket notation they can be dropped under the convention of always working with the set of least positive residues modulo m, replacing each integer by the unique residue to which it is congruent. In subsequent units we shall do this, but for conceptual clarity, we shall persist with the bracket notation in this section.)

You may well be wondering what we hope to gain by introducing this new set of matrices. To signpost the way, recall that our goal is to show that for any positive integer m there is a Fibonacci number u_t such that $m|u_t$, that is, $[u_t] = [0]$. We shall achieve this by finding an integer t such that $[\mathbf{A}^t] = [\mathbf{I}]$, whereupon comparison of the elements in the first row and second column gives the required result.

First we need the following result which essentially says that matrices are multiplied in $M(\mathbb{Z}_m)$ in the normal way, but using the residue class arithmetic.

LEMMA If $\mathbf{X}$ and $\mathbf{Y}$ are matrices in $M(\mathbb{Z})$ then $[\mathbf{X}][\mathbf{Y}] = [\mathbf{XY}]$.

PROOF Let $\mathbf{X} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ and $\mathbf{Y} = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$. Then

$$[\mathbf{XY}] = \left[\begin{pmatrix} x_1y_1 + x_2y_3 & x_1y_2 + x_2y_4 \\ x_3y_1 + x_4y_3 & x_3y_2 + x_4y_4 \end{pmatrix}\right]$$

$$= \begin{pmatrix} [x_1y_1 + x_2y_3] & [x_1y_2 + x_2y_4] \\ [x_3y_1 + x_4y_3] & [x_3y_2 + x_4y_4] \end{pmatrix} \quad \text{(by definition of } [\mathbf{A}]\text{)}$$

$$= \begin{pmatrix} [x_1][y_1] + [x_2][y_3] & [x_1][y_2] + [x_2][y_4] \\ [x_3][y_1] + [x_4][y_3] & [x_3][y_2] + [x_4][y_4] \end{pmatrix} \quad \text{(by definitions of addition and multiplication in } \mathbb{Z}_m\text{)}$$

$$= \begin{pmatrix} [x_1] & [x_2] \\ [x_3] & [x_4] \end{pmatrix} \begin{pmatrix} [y_1] & [y_2] \\ [y_3] & [y_4] \end{pmatrix} = [\mathbf{X}][\mathbf{Y}]. \quad \blacksquare$$

SAQ 21 Use the result of the Lemma to show that $[\mathbf{A}^{-n}]$ is the multiplicative inverse of $[\mathbf{A}^n]$ in $M(\mathbb{Z}_m)$.

SOLUTION TO SAQ 21 To talk about multiplicative inverses we first need an identity element in $M(\mathbb{Z}_m)$. This is plainly $[\mathbf{I}]$, which is confirmed by the Lemma:

$$[\mathbf{X}][\mathbf{I}] = [\mathbf{XI}] = [\mathbf{X}] = [\mathbf{IX}] = [\mathbf{I}][\mathbf{X}].$$

Then,

$$[\mathbf{A}^n][\mathbf{A}^{-n}] = [\mathbf{A}^n\mathbf{A}^{-n}] = [\mathbf{I}] = [\mathbf{A}^{-n}\mathbf{A}^n] = [\mathbf{A}^{-n}][\mathbf{A}^n]$$

shows that $[\mathbf{A}^{-n}] = [\mathbf{A}^n]^{-1}$. $\blacksquare$

And now for the main result.

THEOREM If m is any positive integer then there exists a Fibonacci number u_t such that $m|u_t$.

PROOF We first remark that each matrix in $M(\mathbb{Z}_m)$ has four entries and that each of these entries can take only the m values $[0], [1], \ldots, [m-1]$, so there are in all m^4 distinct matrices in $M(\mathbb{Z}_m)$.

Now consider the matrices

$$[\mathbf{A}], [\mathbf{A}^2], [\mathbf{A}^3], \ldots, [\mathbf{A}^n], \ldots.$$

As there are only a finite number of distinct matrices these cannot all be different. So, focussing on an equal pair, there exist positive integers s and t such that $[\mathbf{A}^s] = [\mathbf{A}^{s+t}]$. That is,

$$[\mathbf{A}^s] = [\mathbf{A}^s][\mathbf{A}^t].$$

Multiplying both sides on the left by $[\mathbf{A}^{-s}]$ gives

$$[\mathbf{A}^t] = [\mathbf{I}].$$

Spelling this out,

$$\begin{pmatrix} [u_{t-1}] & [u_t] \\ [u_t] & [u_{t+1}] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}$$

from which we see that $[u_t] = [0]$ or, what amounts to the same thing, $m|u_t$. ■

Having developed all this machinery it would be a pity not to give further illustration of its powerful applications. To this end, we close the section with an alternative proof of the main Fibonacci divisibility property, namely that $u_m|u_{mn}$ (Theorem 13-2, **B** page 290). To do this we change the modulus of our congruences to u_m, so that we consider matrices in $M(\mathbb{Z}_{u_m})$. In what follows, therefore, the square brackets refer to residue classes and associated matrices modulo u_m, rather than modulo m as previously.

SAQ 22 (a) Show that $[\mathbf{A}^m]$ is a diagonal matrix and hence determine $[\mathbf{A}^m]^n$, where m and n are positive integers.

(b) Use the fact that $[\mathbf{A}^{mn}] = [\mathbf{A}^m]^n$ (which follows from the Lemma) to show that $u_m|u_{mn}$.

SOLUTION TO SAQ 22 (a)

$$\mathbf{A}^m = \begin{pmatrix} [u_{m-1}] & [u_m] \\ [u_m] & [u_{m+1}] \end{pmatrix} = \begin{pmatrix} [u_{m-1}] & [0] \\ [0] & [u_{m+1}] \end{pmatrix}$$

(remember we are now taking congruences modulo u_m).

$$[\mathbf{A}^m]^n = \begin{pmatrix} [u_{m-1}] & [0] \\ [0] & [u_{m+1}] \end{pmatrix}^n = \begin{pmatrix} [u_{m-1}]^n & [0] \\ [0] & [u_{m+1}]^n \end{pmatrix}.$$

(Note further that since $u_{m+1} = u_m + u_{m-1}$, we have $[u_{m+1}] = [u_{m-1}]$ so $[\mathbf{A}^m]^n$ is a scalar multiple of the identity matrix.)

(b) $$[\mathbf{A}^{mn}] = \begin{pmatrix} [u_{mn-1}] & [u_{mn}] \\ [u_{mn}] & [u_{mn+1}] \end{pmatrix}$$

Comparing entries in the first row and second column of $[\mathbf{A}^{mn}]$ and $[\mathbf{A}^m]^n$ we have $[u_{mn}] = [0]$. That is, $u_m|u_{mn}$. ■

3.5 Problem Solving

On the tape cassette accompanying this section we discuss the problems given below. If you feel confident that you can handle these problems without assistance, then by all means go ahead. (Solutions are given in the Exercise Booklet.) However, it should be emphasized that the tape contains much more than just solutions to the problems, and real benefit could be gained from the discussion of the various ways of attacking the problems. In particular, the real purpose of Problem 2 is to suggest a possible strategy for solving linear congruences in general.

START THE TAPE WHEN YOU ARE READY

PROBLEM 1 An integer a is both a square and a cube. Prove that

$$a \equiv 0, 1, 9 \text{ or } 28 \pmod{36}.$$

PROBLEM 2 Solve the following linear congruences.

(i) $28x \equiv 49 \pmod{53}$

(ii) $34x \equiv 19 \pmod{52}$

(iii) $137x \equiv 96 \pmod{19}$

(iv) $51x \equiv 8 \pmod{53}$

(v) $46x \equiv 74 \pmod{98}$

PROBLEM 3 Solve the simultaneous system of congruences

$$2x + 3y \equiv 1 \pmod{100},$$
$$3x - 2y \equiv 1 \pmod{100}.$$

3.6 Summary

This unit has been concerned with the topic of congruence, whose applications we continue to investigate in the next unit and thereafter use extensively in the remainder of the course.

Section 3.1 looked at basic properties of congruence. We found that for each positive integer n there is an arithmetic modulo n which has its own peculiarities. Theorem 4-2 and Theorem 4-3 of **B** give the important rules governing addition, multiplication and cancellation in arithmetic modulo n.

Section 3.2 turned to simple applications of congruence and, in particular, established tests for divisibility by certain integers.

Section 3.3 was concerned with solving linear congruences and solving systems of simultaneous linear congruences. Theorem 4-7 and the Chinese Remainder Theorem gave the respective conditions for solvability, but the section suggested alternative methods of solving each kind of problem.

Section 3.4 returned to the Fibonacci sequence and gave an alternative approach to proving properties of the sequence which used matrix techniques. The power of this approach was illustrated by the comparative ease with which some of the seemingly difficult properties were derived.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

UNIT 4
FERMAT'S THEOREM

4.0 Introduction

The main result of this unit is Fermat's Little Theorem, not to be confused with the probably better known Fermat's Last Theorem which we shall encounter in *Unit 8*. Fermat's Little Theorem states that, when working to prime modulus p, x^{p-1} is congruent to 1 for every integer x which is not divisible by p.

The result has numerous applications, one of the more important of which is its role in the area of solving polynomial congruences, which are congruences of the form $P(x) \equiv 0 \pmod{n}$ where P is a polynomial with integer coefficients. We begin an investigation of polynomial congruences and their solution in Section 4.4. We shall pick up this thread again in *Unit 6* where we carry out a systematic study of the solution of quadratic congruences.

In Section 4.1 we meet an ingenious algorithm for factorizing odd integers, discovered by Fermat. Section 4.2 is concerned with the proof and some simple consequences of Fermat's Little Theorem. Section 4.3 introduces another of the classical results in this area of number theory, known as Wilson's Theorem. Section 4.4 turns to polynomial congruences and is a tape-based section. Finally, in Section 4.5 we take another look at Fermat's and Wilson's Theorems. From their statements, any link between the two theorems must appear tenuous. However, we shall observe certain similarities in their proofs, and in this final section we illustrate how the two results arise out of the solutions of two similar, well-known combinatorial problems.

The unit is based mainly on Chapter 5 of **B**. Section 4.4, however (most of whose material will not be found in **B**), culminates in a short reading passage from Chapter 8.

4.1 Fermat's Factorization Method

To investigate the primality of an integer n, the only method so far presented is to test n systematically for divisibility by each prime not exceeding $\sqrt{n}$, in turn. In this section we shall meet an alternative method: an algorithm discovered by Fermat. Rather than requiring a knowledge of prime numbers, Fermat's method relies on a knowledge of the perfect squares.

But first we learn a little about Fermat himself, one of the great men of number theory.

READ B Chapter 5 from page 92 as far as the end of Section 5.2.

Whilst there is a certain elegance about Fermat's method, it must be said that it is not a very efficient algorithm for factorizing a general integer n. As pointed out in **B**, there are favourable cases for Fermat's Method, occurring when n is a product of two numbers of approximately equal size. But in the vast majority of cases, which are unfavourable, the amount of computation needed to find factors of n by Fermat's method far exceeds that involved in testing n for divisibility by each positive integer not exceeding $\sqrt{n}$.

SAQ 1 **B** page 96, Problems 5.2, number 1, parts (a) and (b).

[Note: **B** contains a list of squares, Table 5 in the Appendices.]

SOLUTION TO SAQ 1 (a) The smallest positive integer k for which $k^2 \geq 2279$ is 48.

$$k^2 - 2279 = 2304 - 2279 = 25 = 5^2$$

Therefore $2279 = (48 + 5) \cdot (48 - 5) = 53 \cdot 43$.

(b) $102^2 < 10541 < 103^2$, so we first take $k = 103$. Writing $n = 10541$,

$$\begin{aligned} 103^2 - n &= 68, \\ 104^2 - n &= 275, \\ 105^2 - n &= 484 = 22^2. \end{aligned}$$

Therefore $n = (105 + 22)\cdot(105 - 22) = 127 \cdot 83$. ■

4.2 Fermat's Little Theorem

The subject matter of this section is one of the classical results of number theory: Fermat's Little Theorem. The theorem is a special case of a more general result, Euler's Theorem, which we shall encounter in *Unit 5*. The usefulness of Fermat's and Euler's Theorems in number theory is difficult to exaggerate.

READ B Section 5.3, page 97, as far as page 99, line −5.

NOTE *Page 98, line 8*
In SAQ 15 of *Unit 3* we proved that $\{0, a, 2a, \ldots, (n-1)a\}$ is a complete set of residues modulo n, provided $\gcd(a, n) = 1$. It follows that for p prime and $p \nmid a$, the integers $a, 2a, 3a, \ldots, (p-1)a$ are congruent modulo p, in some order, to the non-zero elements in the set of least positive residues modulo p. ▲

To further illustrate usage of Fermat's Theorem, let us look at:

EXAMPLE 1 **B** page 102, Problems 5.3, number 10.

(a) For $a \in \{1, 2, 3, \ldots, p-1\}$, $p \nmid a$ and so Fermat's Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$.
Therefore, adding these $p - 1$ congruences,

$$\begin{aligned} 1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} &\equiv 1 + 1 + 1 + \cdots + 1 \\ &\equiv p - 1 \equiv -1 \pmod{p}. \end{aligned}$$

(b) By the Corollary, $a^p \equiv a \pmod{p}$ for all integers a. Therefore

$$\begin{aligned} 1^p + 2^p + 3^p + \cdots + (p-1)^p &\equiv 1 + 2 + 3 + \cdots + (p-1) \\ &\equiv \tfrac{1}{2}p\cdot(p-1), \\ &\equiv p \cdot \left(\frac{p-1}{2}\right) \qquad \left(\frac{p-1}{2} \text{ is an integer, since } p \text{ is odd}\right) \\ &\equiv 0 \pmod{p}. \end{aligned}$$

SAQ 2 Find the remainder when 7^{40} is divided by 17.

SAQ 3 **B** page 101, Problems 5.3, number 8.

SOLUTION TO SAQ 2 By Fermat's Theorem, $7^{16} \equiv 1 \pmod{17}$. Therefore

$$7^{40} = (7^{16})^2 \cdot 7^8 \equiv 1^2 \cdot 7^8 \equiv 7^8 \pmod{17}.$$

Now $7^2 = 49 \equiv -2 \pmod{17}$, and so

$$7^{40} \equiv 7^8 \equiv (7^2)^4 \equiv (-2)^4 \equiv 16 \pmod{17}$$

and the remainder on dividing 7^{40} by 17 is 16. ■

SOLUTION TO SAQ 3 (a) If $\gcd(a, p) = 1$ then $p \nmid a$ and so $a^{p-1} \equiv 1 \pmod p$. Hence if $x = a^{p-2}b$ then $ax = a \cdot a^{p-2} b = a^{p-1} b \equiv b \pmod p$, showing that $a^{p-2} b$ is a solution of $ax \equiv b \pmod p$.

COMMENT In the notation of $\mathbb{Z}_p$ (where the non-zero elements form a group under multiplication), Fermat's Theorem says:

$$[a^{p-1}] = [1], \quad \text{whenever } [a] \neq [0].$$

That is,

$$[a]\,[a^{p-2}] = [1], \quad \text{whenever } [a] \neq [0],$$

so that the non-zero element $[a]$ has multiplicative inverse

$$[a]^{-1} = [a^{p-2}].$$

The linear equation $[a]\,[x] = [b]$ ($[a] \neq [0]$) has unique solution in $\mathbb{Z}_p$

$$[x] = [a]^{-1}\,[b] = [a^{p-2}]\,[b].$$

(b) Since $\gcd(2, 31) = 1$, the congruence $2x \equiv 1 \pmod{31}$ has a unique solution modulo 31 which, by part (a), is $x \equiv 2^{29} \cdot 1 \equiv 2^{29} \pmod{31}$. Now

$$2^{29} = (2^5)^5 \cdot 2^4 = (32)^5 \cdot 2^4 \equiv 1^5 \cdot 2^4 \equiv 16 \pmod{31}$$

and so $x \equiv 16 \pmod{31}$ is the unique solution.

Similarly, $6x \equiv 5 \pmod{11}$ has unique solution $x \equiv 6^9 \cdot 5 \pmod{11}$. Now $6 \equiv -5 \pmod{11}$ and so

$$x \equiv 6^9 \cdot 5 \equiv (-5)^9 \cdot 5 \equiv -1 \cdot 5^{10} \equiv -1 \pmod{11}$$

since $5^{10} \equiv 1 \pmod{11}$ by Fermat's Theorem.

The unique solution of $3x \equiv 17 \pmod{29}$ is

$$\begin{aligned} x &\equiv 3^{27} \cdot 17 \equiv 3^{27} \cdot 17 \cdot 30 \qquad (\text{since } 30 \equiv 1 \pmod{29}) \\ &\equiv 3^{28} \cdot 17 \cdot 10 \equiv 17 \cdot 10 \equiv 25 \pmod{29} \end{aligned}$$

where we have used $3^{28} \equiv 1 \pmod{29}$. ■

READ B from page 99, line -4 to the end of Section 5.3.

NOTES (i) *Page 100, line -9*

The final step in the proof of the lemma follows immediately from our theorem on page 47 of *Unit 3*. It is worthwhile recalling the theorem at this stage for we shall appeal to it several times in what follows.

(ii) *Page 101, line 3*

An alternative way of obtaining the result $2^{340} \equiv 1 \pmod{341}$ is as follows.

By Fermat's Theorem we know that $2^{10} \equiv 1 \pmod{11}$, and so

$$2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}.$$

Further, since $2^5 = 32 \equiv 1 \pmod{31}$, we have

$$2^{340} = (2^5)^{68} \equiv 1^{68} \equiv 1 \pmod{31}.$$

The theorem cited in Note (i) now gives $2^{340} \equiv 1 \pmod{11 \cdot 31}$.

(iii) *Page 101, line 12*

The number 561 is interesting in that, despite being composite, it has the property $a^{560} \equiv 1 \pmod{561}$ for all integers a which are relatively prime to 561 (see SAQ 4). This shows that even if $a^{n-1} \equiv 1 \pmod n$ for *all* integers a with $\gcd(a, n) = 1$, it is still not necessarily the case that n is prime. ▲

The next example further illustrates how we can use Fermat's Theorem in conjunction with the theorem of Note (i) to obtain results about divisibility by composite integers.

XAMPLE 2 **B** page 101, Problems 5.3, number 2.

(a) To show that $a^{12} \equiv 1 \pmod{35}$ it suffices to show that $a^{12} \equiv 1 \pmod 5$ and $a^{12} \equiv 1 \pmod 7$.

Since $\gcd(a, 35) = 1$ we known that $5 \nmid a$ and $7 \nmid a$, so that Fermat's Theorem gives $a^4 \equiv 1 \pmod 5$ and $a^6 \equiv 1 \pmod 7$. Therefore

$$a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \pmod 5,$$

$$a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod 7,$$

as required.

(b) To prove $168 \mid a^6 - 1$ we shall show that $a^6 \equiv 1 \pmod 3$, $a^6 \equiv 1 \pmod 7$ and $a^6 \equiv 1 \pmod 8$. Since 3, 7 and 8 are relatively prime in pairs it will follow that $a^6 \equiv 1 \pmod{3 \cdot 7 \cdot 8}$. Given that $\gcd(a, 42) = 1$ we know that $2 \nmid a$, $3 \nmid a$ and $7 \nmid a$. From the latter, Fermat's Theorem gives $a^6 \equiv 1 \pmod 7$. From $3 \nmid a$ Fermat's Theorem gives $a^2 \equiv 1 \pmod 3$, whence

$$a^6 = (a^2)^3 \equiv 1^3 \equiv 1 \pmod 3.$$

Finally, from $2 \nmid a$ we have that a is odd and so $a^2 \equiv 1 \pmod 8$ (see **B** page 22, third paragraph). But then

$$a^6 = (a^2)^3 \equiv 1 \pmod 8.$$

(c) $133 = 7 \cdot 19$ and so $\gcd(a, 133) = 1$ implies that $7 \nmid a$ and $19 \nmid a$. Employing Fermat's Theorem,

$$a^{18} = (a^6)^3 \equiv 1^3 \equiv 1 \pmod 7 \quad \text{and} \quad a^{18} \equiv 1 \pmod{19}$$

leading to the conclusion that $a^{18} \equiv 1 \pmod{7 \cdot 19}$. Similarly, $b^{18} \equiv 1 \pmod{7 \cdot 19}$, and so $a^{18} - b^{18} \equiv 0 \pmod{7 \cdot 19}$. That is, $133 \mid a^{18} - b^{18}$.

SAQ 4 Show that $a^{560} \equiv 1 \pmod{561}$ whenever $\gcd(a, 561) = 1$.

SAQ 5 **B** page 101, Problems 5.3, number 4.

SAQ 6 For any integer a show that a^5 and a have the same units digit. Deduce that a^{100} has the same units digit as a^4.

SOLUTION TO SAQ 4 $561 = 3 \cdot 11 \cdot 17$ and so if $\gcd(a, 561) = 1$ then $3 \nmid a$, $11 \nmid a$ and $17 \nmid a$. Fermat's Theorem gives $a^2 \equiv 1 \pmod 3$, $a^{10} \equiv 1 \pmod{11}$ and $a^{16} \equiv 1 \pmod{17}$. Therefore,

$$a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod 3,$$

$$a^{560} = (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11},$$

$$a^{560} = (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17},$$

whence $a^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$. ■

SOLUTION TO SAQ 5 (a) By the Corollary to Fermat's Theorem we know

$$a^3 \equiv a \pmod 3 \quad \text{and} \quad a^5 \equiv a \pmod 5.$$

Employing these facts in turn,

$$a^{21} = (a^3)^7 \equiv a^7 \equiv (a^3)^2 a \equiv a^2 a \equiv a^3 \equiv a \pmod 3$$

and

$$a^{21} = (a^5)^4 a \equiv a^4 a \equiv a^5 \equiv a \pmod 5.$$

It follows that $a^{21} \equiv a \pmod{3 \cdot 5}$, as required.

(b) By the Corollary to Fermat's Theorem we know

$$a^2 \equiv a \pmod 2, \quad a^3 \equiv a \pmod 3 \quad \text{and} \quad a^7 \equiv a \pmod 7.$$

The first two give, respectively,

$$a^7 = (a^2)^3 a \equiv a^3 a \equiv a^4 \equiv (a^2)^2 \equiv a^2 \equiv a \pmod{2}$$

and

$$a^7 = (a^3)^2 a \equiv a^2 a \equiv a^3 \equiv a \pmod{3}.$$

Now $a^7 \equiv a \pmod{2 \cdot 3 \cdot 7}$, as required.

(c) (Similar to (b).) From $a^3 \equiv a \pmod{3}$ we deduce that

$$a^{13} = (a^3)^4 a \equiv a^4 a \equiv a^3 a^2 \equiv aa^2 \equiv a^3 \equiv a \pmod{3}$$

and from $a^7 \equiv a \pmod{7}$ we obtain

$$a^{13} = a^7 a^6 \equiv aa^6 \equiv a^7 \equiv a \pmod{7}.$$

Not forgetting $a^{13} \equiv a \pmod{13}$, we conclude that $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$. ■

SOLUTION TO SAQ 6 Two integers have the same units digit if, and only if, they are congruent modulo 10. For any integer a we have $a^5 \equiv a \pmod{5}$ and $a^2 \equiv a \pmod{2}$. From the latter,

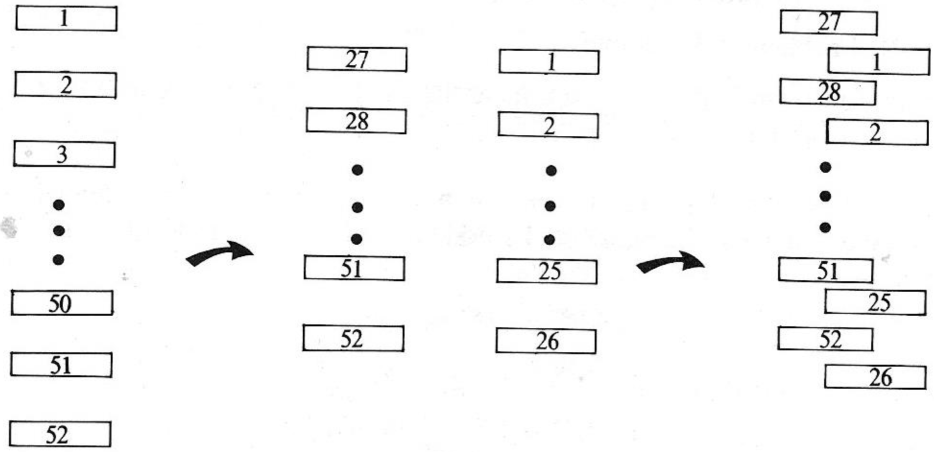
$$a^5 = (a^2)^2 a \equiv a^2 a \equiv a^2 \equiv a \pmod{2},$$

and therefore $a^5 \equiv a \pmod{10}$, as required.

$$\begin{aligned} a^{100} = (a^5)^{20} &\equiv a^{20} \qquad (\text{since } a^5 \equiv a \pmod{10}) \\ &\equiv (a^5)^4 \equiv a^4 \pmod{10} \end{aligned}$$

and so a^{100} has the same units digit as a^4. ■

EXAMPLE 3 Consider an ordinary pack of 52 playing cards in any order. In the perfect faro shuffle the pack is cut into two equal halves which are then placed (flicked) alternately, as illustrated.



After how many such shuffles will the pack return to its original order?

The cards which initially occupy positions $1, 2, \ldots, 26$ are moved to positions $2, 4, \ldots, 52$, whilst the cards initially in positions $27, 28, \ldots, 52$ are moved to positions $1, 3, \ldots, 51$. Thus the card starting in position x ends up in position y where $1 \leq y \leq 52$ and $y \equiv 2x \pmod{53}$. After n such shuffles this card will occupy position $2^n x \pmod{53}$.

If all cards return to their initial positions after n shuffles then

$$2^n x \equiv x \pmod{53}, \text{ for all } x \text{ such that } 1 \leq x \leq 52.$$

As 53 is prime we may cancel x to obtain

$$2^n \equiv 1 \pmod{53}.$$

Now Fermat's Theorem gives us one positive value of n which satisfies this congruence: $2^{52} \equiv 1 \pmod{53}$. Hence after 52 shuffles the pack is restored to its original order.

In fact $n = 52$ is the least positive solution of $2^n \equiv 1 \pmod{53}$ (see SAQ 7), so the pack returns to its original order for the first time after the 52nd shuffle.

Suppose now that we take a pack of m cards (where m is even) and apply perfect faro shuffles as before. The rules governing the movement of the cards are just as in the above example. After n shuffles the card which originally occupied position x is moved to position y where $1 \leq y \leq m$ and $y \equiv 2^n x \pmod{m+1}$. The pack returns to its original order after n shuffles if and only if

$$2^n x \equiv x \pmod{m+1}, \text{ for all } x \text{ such that } 1 \leq x \leq m.$$

Take for example the case $m = 62$. Since

$$2^6 = 64 \equiv 1 \pmod{63}$$

we have

$$2^6 x \equiv x \pmod{63} \text{ for all } x \text{ such that } 1 \leq x \leq 62.$$

Therefore, for a pack of 62 cards, after only 6 shuffles the original order is restored.

SAQ 7 Let $n = n_0$ be the least positive solution of $2^n \equiv 1 \pmod{53}$. Use the Division Algorithm to show that $n_0 | 52$. Confirm that $2^{26} \not\equiv 1 \pmod{53}$ and deduce that $n_0 = 52$.

SAQ 8 Two jokers are added to an ordinary pack of playing cards. After how many perfect faro shuffles does the resulting pack of 54 cards return to its original order?

OLUTION TO SAQ 7 From the Division Algorithm we can write $52 = qn_0 + r$, where $0 \leq r < n_0$. Now $2^{52} \equiv 2^{n_0} \equiv 1 \pmod{53}$ and so

$$1 \equiv 2^{52} \equiv 2^{qn_0+r} \equiv (2^{n_0})^q \cdot 2^r \equiv 1^q \cdot 2^r \equiv 2^r \pmod{53}.$$

Hence $r = 0$, for otherwise we contradict the definition of n_0 as least positive integer with this property, and therefore $n_0 | 52$.

The possible values of n_0, being a divisor of 52, are 1, 2, 4, 13, 26 or 52. The first three of these can be eliminated at once since clearly they do not satisfy $2^n \equiv 1 \pmod{53}$. Turning to 26,

$$2^{26} = (2^6)^4 \cdot 2^2 \equiv 11^4 \cdot 4 \equiv (11^2)^2 \cdot 4 \equiv 15 \cdot 15 \cdot 4 \equiv 15 \cdot 7 \equiv -1 \pmod{53}.$$

Finally, suppose $2^{13} \equiv 1 \pmod{53}$. Then $2^{26} = (2^{13})^2 \equiv 1^2 \equiv 1 \pmod{53}$, a contradiction. We conclude that $n_0 = 52$. ■

OLUTION TO SAQ 8 The pack of 54 cards returns to its initial order after n shuffles provided $2^n x \equiv x \pmod{55}$, for all x such that $1 \leq x \leq 54$. Since $\gcd(2^n, 55) = 1$ for all $n \geq 1$, x may be cancelled and the required condition is $2^n \equiv 1 \pmod{55}$.

Now $55 = 5 \ 11$, and by Fermat's Theorem we know that $2^4 \equiv 1 \pmod{5}$ and $2^{10} \equiv 1 \pmod{11}$. Therefore

$$2^{20} = (2^4)^5 \equiv 1^5 \equiv 1 \pmod{5}$$

and

$$2^{20} = (2^{10})^2 \equiv 1^2 \equiv 1 \pmod{11},$$

and so $2^{20} \equiv 1 \pmod{5 \cdot 11}$, giving $n = 20$ as a solution to our problem.

If there is a smaller solution than $n = 20$ then, as in SAQ 7, it must be a divisor of 20. But $2^{10} = 1024 \equiv 34 \pmod{53}$, and the other divisors are easily eliminated. ■

4.3 Wilson's Theorem

In the proof of Fermat's Theorem we compared the product of the elements in a complete set of residues modulo p, excluding the element which is congruent to 0, with the product of the numbers $1, 2, \dots, p-1$. Observing that the two products are congruent modulo p, the latter being $(p-1)!$, led to the result. More careful examination of the product $1 \cdot 2 \cdot 3 \dots (p-1)$ reveals that, with the exception of 1 and $p-1$, the elements in the product break into disjoint pairs in such a way that the product of each pair is congruent to 1 modulo p. From this it is a short step to deduce that $(p-1)! \equiv -1 \pmod{p}$, a result known as Wilson's Theorem.

READ B Section 5.4, page 102, as far as page 104, line −11.

NOTE *Page 103, line 16*
In SAQ 3 we showed that the unique solution $x = a'$ of the congruence $ax \equiv 1 \pmod{p}$ is given by $a' \equiv a^{p-2} \pmod{p}$. In terms of $\mathbb{Z}_p$, the non-zero elements $\{[1], [2], \dots, [p-1]\}$ form a group under multiplication and so each element has an inverse, and $[a]^{-1} = [a'] = [a^{p-2}]$. The next part of the proof observes that, with the exception of $[1]$ and $[p-1]$, each element is distinct from its inverse, whereas $[1]^{-1} = [1]$ and $[p-1]^{-1} = [p-1]$. ▲

As an illustration of the use of Wilson's Theorem let us look at:

EXAMPLE 4 **B** page 107, Problems 5-4, number 9.

Working modulo p, where p is an odd prime, we have

$$2 \equiv -(p-2),\ 4 \equiv -(p-4), \dots,\quad 2k \equiv -(p-2k), \dots,\quad p-1 \equiv -1.$$

So the even integers $2, 4, 6, \dots, p-1$ are congruent modulo p respectively to the negatives of the odd integers, $-(p-2), -(p-4), \dots, -5, -3, -1$. Taking their product,

$$\begin{aligned} 2 \cdot 4 \cdot 6 \dots (p-1) &\equiv -1 \cdot -3 \cdot -5 \dots -(p-2) \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdot 5 \dots (p-2) \pmod{p}. \end{aligned}$$

Now utilize Wilson's Theorem:

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdot 3 \dots (p-2)(p-1) \\ &\equiv (1 \cdot 3 \cdot 5 \dots (p-2))\,(2 \cdot 4 \cdot 6 \dots (p-1)) \\ &\equiv (-1)^{\frac{p-1}{2}} (1 \cdot 3 \cdot 5 \dots (p-2))^2 \pmod{p}. \end{aligned}$$

Multiplying both sides by $(-1)^{\frac{p-1}{2}}$, we conclude that

$$1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

SAQ 9 **B** page 106, Problems 5.4, number 3.

SAQ 10 **B** page 106, Problems 5.4, number 1.

SAQ 11 **B** page 106, Problems 5.4, number 4.

SOLUTION TO SAQ 9 The above note suggested a systematic, though rather cumbersome, method of solving this problem. For each integer a we determine a^{-1} from $a^{-1} \equiv a^{p-2} \pmod{p}$. However, you should have been able to 'spot' the ten pairs corresponding to $p = 23$, particularly after making the following observation. If $ab \equiv 1 \pmod{p}$ then $(-a)(-b) \equiv 1 \pmod{p}$, and so $(p-a)(p-b) \equiv 1 \pmod{p}$.

For example, seeing that $4 \cdot 6 \equiv 1 \pmod{23}$, we deduce immediately that

$$(23-4)\cdot(23-6) = 19 \cdot 17 \equiv 1 \pmod{23}.$$

From the divisors of 24 ($\equiv 1 \pmod{23}$) we have the pairs

$$2 \cdot 12 \equiv 3 \cdot 8 \equiv 4 \cdot 6 \equiv 1 \pmod{23}$$

and these give, as above,

$$21 \cdot 11 \equiv 20 \cdot 15 \equiv 19 \cdot 17 \equiv 1 \pmod{23}.$$

Since $70 \equiv 1 \pmod{23}$, we have the further pairs

$$5 \cdot 14 \equiv 7 \cdot 10 \equiv 1 \pmod{23}$$

and, subtracting from 23,

$$18 \cdot 9 \equiv 16 \cdot 13 \equiv 1 \pmod{23},$$

completing the list. ■

OLUTION TO SAQ 10 (a) In the proof of Wilson's Theorem we established that $(p-2)! \equiv 1 \pmod{p}$, for p prime. Putting $p = 17$ gives $15! \equiv 1 \pmod{17}$. That is, the remainder on dividing $15!$ by 17 is 1.

(b) If $p > 3$ is prime, then

$$2(p-3)! \equiv -(p-2)(p-3)! \equiv -(p-2)! \equiv -1 \pmod{p}.$$

Putting $p = 29$ gives

$$2 \cdot 26! \equiv -1 \pmod{29}$$

and so the remainder on dividing $2 \cdot 26!$ by 29 is 28. ■

OLUTION TO SAQ 11 $437 = 19 \cdot 23$. To show that $18! \equiv -1 \pmod{437}$ it is sufficient to show that $18! \equiv -1 \pmod{19}$ and $18! \equiv -1 \pmod{23}$. The former is given immediately by Wilson's Theorem.

Working modulo 23, Wilson's Theorem gives

$$\begin{aligned} -1 \equiv 22! &\equiv 18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \\ &\equiv 18! \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \equiv 18! \cdot 24 \equiv 18! \pmod{23}. \end{aligned}$$ ■

In the final reading passage of this section, quadratic congruences are introduced. As we shall shortly see, the theory of quadratic congruences has great importance in number theory, and *Unit 6* of this course is devoted to their study. The result of Theorem 5-3 is crucial in this context and we shall refer back to it several times in the later units.

READ B from page 104, line -10 to the end of Section 5.4.

NOTE *Page 106, line 10*
Wilson's Theorem tells us that $p \mid (p-1)! + 1$. Putting $n = p - 1$ gives $n + 1 \mid n! + 1$. As $n! + 1 > n + 1$ provided $n > 2$, we conclude that $n! + 1$ is composite whenever $n + 1$ is a prime greater than 3. ▲

For an application of Theorem 5-3 look at

XAMPLE 5 **B** page 107, Problems 5.4, number 12.

This exercise gives us a partial result *en route* to solving a classical problem, which we shall look at in more detail in *Unit 8*, namely, 'which positive integers can be expressed as the sum of two squares?' For example, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$ and $13 = 2^2 + 3^2$ can be so expressed. If you experiment with the numbers in the range 1 to 10 inclusive you will find that the only ones which cannot be expressed as a sum of two squares are 3, 6 and 7. Notice that each of these has a prime factor of the form $4k + 3$.

The result of the present exercise can be re-interpreted as follows. If $p = 4k + 3$ is prime and if a multiple of p can be expressed as a sum of two squares ($a^2 + b^2 \equiv 0 \pmod{p}$), then $p|a$ and $p|b$. But we can take this an immediate step further, for if $p|a$ and $p|b$ then $p^2|a^2 + b^2$. This means that an integer which is a multiple of p but which is not a multiple of p^2 cannot be expressed as a sum of two squares. This accounts for the failure with integers 3, 6 and 7.

Having sketched the background to the problem, its solution presents little difficulty, thanks to Theorem 5-3.

Suppose $a^2 + b^2 \equiv 0 \pmod{p}$ and assume $p \nmid a$. As in the proof of Wilson's Theorem, a has an inverse, that is, an integer c such that $ac \equiv 1 \pmod{p}$. Multiplying through the original congruence by c^2 gives

$$a^2c^2 + b^2c^2 \equiv 0 \cdot c^2 \equiv 0 \pmod{p}$$

or

$$1 + (bc)^2 \equiv 0 \pmod{p},$$

telling us that bc is a solution of $1 + x^2 \equiv 0 \pmod{p}$. But this congruence has no solutions, by Theorem 5-3. The existence of the integer c is thereby contradicted, and we must have $p|a$. Similarly, by the symmetry of the situation, $p|b$.

SAQ 12 **B** page 107, Problems 5.4, number 11.

SAQ 13 **B** page 107, Problems 5.4, number 10.

SOLUTION TO SAQ 12 From the proof of Theorem 5-3 we know that, for $p \equiv 1 \pmod{4}$, the congruence $x^2 \equiv -1 \pmod{p}$ has solution $x \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$. Further, since $(-1)^2 = 1$, it is clear that $x \equiv -\left(\frac{p-1}{2}\right)! \pmod{p}$ is a second solution. These two solutions are incongruent modulo p (for $x \equiv -x \pmod{p}$ leads to $x \equiv 0 \pmod{p}$, which is not the case), and as we shall discover in the next section these two are in fact the only solutions.

Our task is therefore to simplify the values $\pm\left(\frac{p-1}{2}\right)! \pmod{p}$ for the cases $p = 29$ and $p = 37$.

For $p = 29$, $\left(\frac{p-1}{2}\right)! = 14!$ Working modulo 29 we can simplify 14! by pairing the terms:

$$\begin{aligned} 14! &= 1 \cdot (2 \cdot 14) \cdot (3 \cdot 10) \cdot (4 \cdot 7) \cdot (5 \cdot 6) \cdot (8 \cdot 11) \cdot (9 \cdot 13) \cdot 12 \\ &\equiv 1 \cdot -1 \cdot 1 \cdot -1 \cdot 1 \cdot 1 \cdot 1 \cdot 12 \equiv 12 \pmod{29}. \end{aligned}$$

So two solutions of $x^2 + 1 \equiv 0 \pmod{29}$ are $x \equiv 12 \pmod{29}$ and $x \equiv -12 \equiv 17 \pmod{29}$.

For $p = 37$ the required solutions are $x \equiv \pm 18! \pmod{37}$, which simplify to $x \equiv 6, 31 \pmod{37}$. [It is not unreasonable to 'spot' the solution 6 here, giving $-6 \equiv 31 \pmod{37}$ as the second solution.] ■

SOLUTION TO SAQ 13 (a) Retrace the argument on **B** page 105, starting at line 6. For the case $p = 4k + 3$, the argument differs on line -5 where $(-1)^{(p-1)/2} = -1$, giving

$$1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}.$$

We conclude that $\left(\dfrac{p-1}{2}\right)!$ satisfies the congruence $x^2 \equiv 1 \pmod{p}$. But $x \equiv \pm 1 \pmod{p}$ are the only solutions of this congruence (see the second paragraph of the proof of Wilson's Theorem on **B** page 103), and so either $\left(\dfrac{p-1}{2}\right)! \equiv 1 \pmod{p}$ or $\left(\dfrac{p-1}{2}\right)! \equiv -1 \pmod{p}$.

(b) Consider the product of all the even integers less than p:

$$\begin{aligned} 2\cdot 4\cdot 6\ldots(p-1) &= 2^{(p-1)/2}\cdot 1\cdot 2\cdot 3\ldots\left(\frac{p-1}{2}\right) \\ &= 2^{(p-1)/2}\cdot\left(\frac{p-1}{2}\right)! \\ &= \pm\, 2^{(p-1)/2} \pmod{p}, \qquad \text{by part (a).} \end{aligned}$$

Now Fermat's Theorem tells us that $2^{p-1} \equiv 1 \pmod{p}$, and so

$$(2^{(p-1)/2})^2 \equiv 1 \pmod{p}.$$

But the only solutions of $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$ and so $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Therefore

$$2\cdot 4\cdot 6\ldots(p-1) \equiv \pm 1 \ (\mathrm{mod}\, p = 4k+3)$$

as required. ■

4.4 Polynomial Congruences

What values of x satisfy

$$x^{20} + 3x^{14} + 8x^{10} + 3x^2 + 6 \equiv 0 \pmod{7}?$$

To solve a congruence such as this may, at first sight, appear to be an awkward task. But Fermat's Theorem leads to immediate simplifications.

If $x \equiv 0 \pmod{7}$ then the left-hand side of the congruence is clearly seen to be congruent to 6 modulo 7, and so no x which is a multiple of 7 can be a solution of the congruence. Therefore in looking for solutions we may assume that $7 \nmid x$, which permits us to apply Fermat's Theorem, namely that $x^6 \equiv 1 \pmod{7}$. Then

$$x^{20} = (x^6)^3\cdot x^2 \equiv 1^3\cdot x^2 \equiv x^2 \pmod{7}.$$

Similarly, $x^{14} \equiv x^2 \pmod{7}$ and $x^{10} \equiv x^4 \pmod{7}$. Therefore solving the original congruence is equivalent to solving

$$x^2 + 3x^2 + 8x^4 + 3x^2 + 6 = 8x^4 + 7x^2 + 6 \equiv 0 \pmod{7}.$$

Simplifying further by reducing the coefficients ($8 \equiv 1 \pmod{7}$, etc.), we arrive at

$$x^4 - 1 \equiv 0 \pmod{7}.$$

Checking the fourth powers of ± 1, ± 2 and ± 3 we find that this congruence has just two solutions, namely $x \equiv \pm 1 \pmod{7}$. These two are also the solutions of the original congruence.

This example illustrates an important role played by Fermat's Theorem towards the solution of 'polynomial congruences', enabling us to replace the polynomial in question by an equivalent one of smaller degree. In this section we are going to be wholly concerned with polynomial congruences and their solutions. We shall discover that when the modulus of the congruence is composite, unexpected and unwanted things happen. But when the modulus is prime the situation is more clear-cut.

The culmination of the section is a theorem of Lagrange which gives an insight into the number of solutions that a polynomial congruence with prime modulus can have.

START THE TAPE WHEN YOU ARE READY

FRAME 1 Definitions

A *polynomial congruence* is an expression

$$P(x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{n}$$

where P is an *integral polynomial* (that is, a polynomial whose coefficients are integers).

Integer b is a solution of $P(x) \equiv 0 \pmod{n}$ if and only if $P(b) \equiv 0 \pmod{n}$.

The number of solutions of $P(x) \equiv 0 \pmod{n}$ is the number of incongruent solutions modulo n. That is, the number of solutions in a complete set of residues, for example $\{0, 1, 2, \ldots, n-1\}$.

FRAME 2 Degree

The *degree* of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ is defined as the highest exponent in P whose coefficient is not congruent to 0 modulo n.

Examples

(i) $3x^6 - x^3 + 2 \equiv 0 \pmod{4}$ has degree 6

(ii) $5x^4 + 6x^3 + 17x \equiv 0 \pmod{5}$ has degree 3

(iii) $6x^3 + 3x^2 + 9x + 2 \equiv 0 \pmod{3}$ has degree 0

(iv) $7x^2 - 14x + 7 \equiv 0 \pmod{7}$ has degree ?

A polynomial all of whose coefficients are congruent to 0 modulo n (the zero polynomial over $\mathbb{Z}_n$) has no degree associated with it.

FRAME 3 Examples of solutions modulo 3

$P(x)$	$P(0)$	$P(1)$	$P(2)$	Solutions of $P(x) \equiv 0 \pmod{3}$
$x^2 - 1$	2	0	0	1, 2
$x^2 + 1$	1	2	2	None
$x^2 + x + 1$	1	0	1	1
$4x^2 + 2$	2	0	0	1, 2
$x^3 - x$	0	0	0	0, 1, 2
$x^3 + x^2 + 2x + 2$	2	0	0	1, 2

FRAME 4 Congruent polynomials

Polynomials P_1 and P_2 are said to be *congruent* modulo n if and only if they take the same value at each integer. That is, $P_1(x) \equiv P_2(x) \pmod{n}$ for each integer x.

Examples

$x^3 + x^2 + 2x + 2 \equiv 4x^2 + 2 \pmod{3}$

$10x^3 - 2x^2 + 7 \equiv 3x^2 + 2 \pmod{5}$ (Here corresponding coefficients are congruent modulo 5.)

FRAME 5 SAQ 14

Use Fermat's Theorem to show that

$$x^6 + 2x^5 + x^4 - 2x^3 - x^2 - 1 \equiv x^4 + 3x^3 + 2x + 4 \pmod{5}.$$

FRAME 6 SAQ 15

Solve the polynomial congruences

(i) $x^3 - x \equiv 0 \pmod{6}$,

(ii) $x^2 - 1 \equiv 0 \pmod{8}$,

(iii) $x^5 - x^3 \equiv 0 \pmod{8}$,

(iv) $x^3 - 1 \equiv 0 \pmod{7}$,

(v) $x^2 + x + 1 \equiv 0 \pmod{7}$.

RAME 6A Solution to SAQ 15

(i) By the Corollary to Fermat's Theorem, $x^3 \equiv x \pmod{3}$ for all x. But $x^3 \equiv x \pmod{2}$, and so $x^3 \equiv x \pmod{2 \cdot 3}$. That is, $x^3 - x \equiv 0 \pmod{6}$ has solutions $x \equiv 0, 1, 2, 3, 4$ and $5 \pmod{6}$.

(ii) $x^2 \equiv 1 \pmod{8}$ if and only if x is odd. (See **B** page 22, paragraph 3.) Therefore $x \equiv 1, 3, 5$ and $7 \pmod{8}$ are the solutions.

(iii) $x^5 - x^3 = x^3(x^2 - 1) \equiv 0 \pmod{8}$

$x \equiv 1, 3, 5, 7 \pmod{8} \implies x^2 - 1 \equiv 0 \pmod{8}$

$x \equiv 0, 2, 4, 6 \pmod{8} \implies x^3 \equiv 0 \pmod{8}$

Therefore $x^5 - x^3 \equiv 0 \pmod{8}$ for all integers x.

(iv) $x \equiv 1, 2, 4 \pmod{7}$ all have $x^3 \equiv 1 \pmod{7}$, and these are the three solutions.

(v) Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, any solution of $x^2 + x + 1 \equiv 0 \pmod{7}$ must also be a solution of $x^3 - 1 \equiv 0 \pmod{7}$, of which there are three, found in part (iv). Trying $x \equiv 1, 2, 4 \pmod{7}$ we find that $x \equiv 2, 4 \pmod{7}$ are the solutions of $x^2 + x + 1 \equiv 0 \pmod{7}$. ■

FRAME 7 Factorizing polynomial congruences

(i) Composite modulus

$$x^3 - x \equiv 0 \pmod{6} \iff x \equiv 0, 1, 2, 3, 4, 5 \pmod{6}.$$

But

$$\begin{tikzcd}[column sep=small] x^3 - x = x(x^2 - 1) = x \arrow[d] & (x - 1) \arrow[d] & (x + 1) \equiv 0 \pmod{6} \arrow[d] \\ x \equiv 0 \pmod{6} & x \equiv 1 \pmod{6} & x \equiv 5 \pmod{6} \end{tikzcd}$$

(ii) Prime modulus

(a) $x^2 + x + 1 \equiv 0 \pmod{7} \iff x \equiv 2, 4 \pmod{7}$

$(x - 2)(x - 4) = x^2 - 6x + 8 \equiv x^2 + x + 1 \pmod{7}$

(b) $x^3 - 1 \equiv 0 \pmod{7} \iff x \equiv 1, 2, 4 \pmod{7}$

$x^3 - 1 = (x - 1)(x^2 + x + 1) \equiv (x - 1)(x - 2)(x - 4) \pmod{7}$

FRAME 8 Roots of polynomials

If x_1 is a root of polynomial $P(x)$ then

$$P(x) = (x - x_1)P(x).$$

If x_2 is a second root, $x_2 \neq x_1$, then

$$P(x_2) = (x_2 - x_1)P_1(x_2) = 0$$

so that $P_1(x_2) = 0$. Therefore

$$P_1(x) = (x - x_2)P_2(x)$$

giving

$$P(x) = (x - x_1)(x - x_2)P_2(x).$$

Continuing,

$$P(x) = (x - x_1)(x - x_2)\ldots(x - x_r)P_r(x)$$

shows that if P has more than n roots then the degree of P must exceed n.

Example

1, -2 and 3 are roots of

$$P(x) = 3x^4 - 9x^3 - 9x^2 + 33x - 18.$$

Therefore $P(x) = (x - 1)P_1(x)$, where

$$P_1(x) = 3x^3 - 6x^2 - 15x + 18.$$

Now $P_1(x) = (x + 2)P_2(x)$, where

$$\begin{aligned} P_2(x) &= 3x^2 - 12x + 9 \\ &= (x - 3)P_3(x), \text{ where} \end{aligned}$$

$$P_3(x) = 3x - 3.$$

Therefore

$$P(x) = (x - 1)(x + 2)(x - 3)(3x - 3).$$

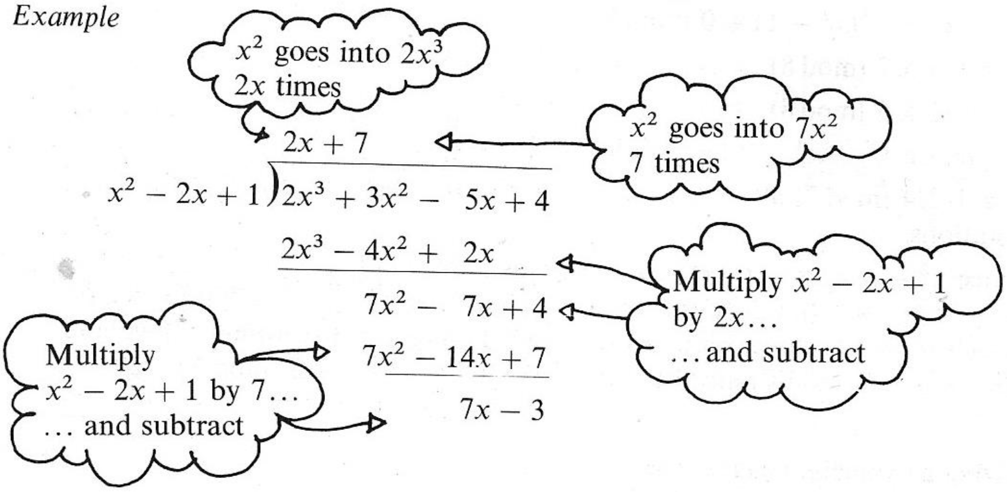
FRAME 9 Division Algorithm for polynomials

Given polynomials $a(x)$ and $b(x)$ there exist polynomials $q(x)$ and $r(x)$ such that

$$a(x) = q(x) \cdot b(x) + r(x)$$

where $r(x) = 0$ or the degree of r is less than the degree of b.

Example



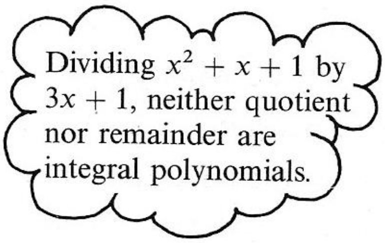
$$\begin{array}{r l}
 & 2x + 7 \\ \hline
x^2 - 2x + 1 \,\big) & 2x^3 + 3x^2 - 5x + 4 \\
 & 2x^3 - 4x^2 + 2x \\ \hline
 & 7x^2 - 7x + 4 \\
 & 7x^2 - 14x + 7 \\ \hline
 & 7x - 3
\end{array}$$

x^2 goes into $2x^3$ $2x$ times
x^2 goes into $7x^2$ 7 times
Multiply $x^2 - 2x + 1$ by $2x$... ...and subtract
Multiply $x^2 - 2x + 1$ by 7... ... and subtract

$$2x^3 + 3x^2 - 5x + 4 = (2x + 7) \cdot (x^2 - 2x + 1) + 7x - 3$$

BUT...

$$\begin{array}{r l}
 & \tfrac{1}{3}x + \tfrac{2}{9} \\ \hline
3x + 1 \,\big) & x^2 + x + 1 \\
 & x^2 + \tfrac{1}{3}x \\ \hline
 & \tfrac{2}{3}x + 1 \\
 & \tfrac{2}{3}x + \tfrac{2}{9} \\ \hline
 & \tfrac{7}{9}
\end{array}$$



Dividing $x^2 + x + 1$ by $3x + 1$, neither quotient nor remainder are integral polynomials.

FRAME 10 Theorem

If $a(x)$ and $b(x)$ are integer polynomials with the leading coefficient of $b(x)$ equal to 1, then there exist integer polynomials $q(x)$ and $r(x)$ such that

$$a(x) = q(x) \cdot b(x) + r(x)$$

where $r(x) = 0$ or degree $r(x) <$ degree $b(x)$.

Proof

Consider the set S of integer polynomials

$$S = \{a(x) - c(x) \cdot b(x) : c(x) \text{ any integer polynomial}\}.$$

If the zero polynomial belongs to S, then $a(x) = c(x) \cdot b(x) + 0$, for some integer polynomial $c(x)$, and this is of the required form. Otherwise, let $r(x)$ be a polynomial in S having least degree, say

$$r(x) = a(x) - q(x) \cdot b(x)$$

i.e.

$$a(x) = q(x) \cdot b(x) + r(x).$$

We shall show that degree $r(x) <$ degree $b(x)$ by contradiction. If

degree $r(x) \geq$ degree $b(x)$ then

$$b(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

and

$$r(x) = r_1x^{m+s} + r_2x^{m+s-1} + \cdots, \text{where } s \geq 0.$$

Consider $a(x) - (q(x) + r_1x^s)b(x)$, which belongs to S.

$$\begin{aligned} a(x) - (q(x) + r_1x^s)b(x) & \\ &= r(x) - r_1x^sb(x) \\ &= r_1x^{m+s} + r_2x^{m+s-1} + \cdots - (r_1x^{m+s} + r_1b_{m-1}x^{m+s-1} + \cdots) \\ &= (r_2 - r_1b_{m-1})x^{m+s-1} + \cdots. \end{aligned}$$

This member of S has degree less than $m + s$, which contradicts the fact that $r(x)$ has least degree. ■

READ B from Theorem 8-5 on page 162 to page 164, line -11.

FRAME 11 Note on Lagrange's Theorem

From examples seen, we know that the condition p be prime is essential. Indeed, working to any composite modulus n we can always find a polynomial of degree 1 for which the corresponding congruence has at least two incongruent solutions. For, if $n = ab$ where $1 < a \leq b < n$ then the congruence $ax + c \equiv 0 \pmod{n}$ has $\gcd(a, n) = a$ incongruent solutions, whenever $a \mid c$.

This observation pinpoints the first place where the primality of p is needed in the proof of Lagrange's Theorem. The case $n = 1$, launching the induction, is false for composite p. The primality is needed once more, on page 163, lines 7 and 8. Arriving at $(b - a)q(b) \equiv 0 \pmod{p}$ and $p \nmid b - a$, Theorem 3-1 (**B** page 47) gives $p \mid q(b)$ so that we deduce $q(b) \equiv 0 \pmod{p}$, as required.

END OF TAPE

SAQ 16 Find the quotient and remainder when $a(x)$ is divided by $b(x)$, where

(i) $a(x) = 2x^3 - x + 1, \quad b(x) = x + 1;$

(ii) $a(x) = 2x^4 - 1, \quad b(x) = x^2 - x - 1.$

SAQ 17 Solve the following congruences.

(i) $x^3 - 2x + 1 \equiv 0 \pmod{11}$

(ii) $x^{10} - x^8 + 5x^3 - 5x \equiv 0 \pmod{7}$

SAQ 18 Prove that the congruence

$$x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p},$$

where p is an odd prime, has exactly $p - 2$ incongruent solutions, which are

$$x \equiv 2, 3, \ldots, p - 1 \pmod{p}.$$

SOLUTION TO SAQ 16 (i)

$$\begin{array}{r|rrrr}
 & 2x^2 & -2x & +1 & \\ \cline{2-5}
x+1 & 2x^3 & & -x & +1 \\
 & 2x^3 & +2x^2 & & \\ \cline{2-5}
 & & -2x^2 & -x & +1 \\
 & & -2x^2 & -2x & \\ \cline{2-5}
 & & & x & +1 \\
 & & & x & +1 \\ \cline{2-5}
 & & & & 0
\end{array}$$

$q(x) = 2x^2 - 2x + 1$

$r(x) = 0$

(ii)

$$\begin{array}{r|rrrrr}
 & 2x^2 & +2x & +4 & & \\ \cline{2-6}
x^2 - x - 1 & 2x^4 & & & & -1 \\
 & 2x^4 & -2x^3 & -2x^2 & & \\ \cline{2-6}
 & & 2x^3 & +2x^2 & & -1 \\
 & & 2x^3 & -2x^2 & -2x & \\ \cline{2-6}
 & & & 4x^2 & +2x & -1 \\
 & & & 4x^2 & -4x & -4 \\ \cline{2-6}
 & & & & 6x & +3
\end{array}$$

$q(x) = 2x^2 + 2x + 4$

$r(x) = 6x + 3 \quad \blacksquare$

SOLUTION TO SAQ 17 (i) Noticing that $x \equiv 1 \pmod{11}$ is one solution, we can factorize

$$\begin{aligned}
x^3 - 2x + 1 &= (x - 1)(x^2 + x - 1) \\
&\equiv (x - 1)(x^2 + x - 12) \\
&\equiv (x - 1)(x - 3)(x + 4) \equiv 0 \pmod{11}.
\end{aligned}$$

Therefore $x \equiv 1 \pmod{11}$, $x \equiv 3 \pmod{11}$ and $x \equiv -4 \equiv 7 \pmod{11}$ are solutions, and by Lagrange's Theorem, these are the only solutions.

(ii) We first simplify the congruence, using the fact that $x^7 \equiv x \pmod{7}$, for all x. This gives

$$x^4 + 5x^3 - x^2 - 5x = x(x^3 + 5x^2 - x - 5) \equiv 0 \pmod{7}.$$

Spotting that $x = 1$ is a root of the second factor,

$$\begin{aligned} x(x^3 + 5x^2 - x - 5) &= x(x-1)(x^2 + 6x + 5) \\ &\equiv x(x-1)(x^2 - x - 2) \\ &\equiv x(x-1)(x+1)(x-2) \equiv 0 \pmod{7}. \end{aligned}$$

As the original congruence is equivalent to one of degree 4, Lagrange's Theorem tells us that the resulting four solutions, $x \equiv 0, 1, 2$ and $6 \pmod{7}$, are the only solutions. ■

SOLUTION TO SAQ 18 By Fermat's Theorem, each of the integers $1, 2, \ldots, p-1$ is a solution of the congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$. Now

$$x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1).$$

Since none of the integers $2, 3, \ldots, p-1$ satisfy $x - 1 \equiv 0 \pmod{p}$ it follows, by the proof of Lagrange's Theorem, that each of them is a solution of $x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$. ■

4.5 Fermat's and Wilson's Theorems Revisited

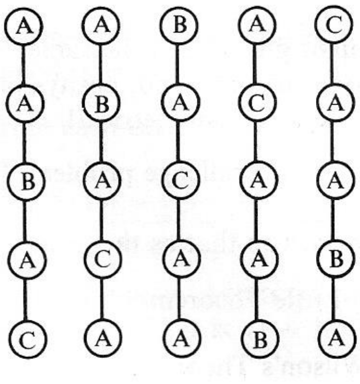
The results of Fermat's and Wilson's Theorems are illustrated in the solutions of two well-known combinatorial problems.

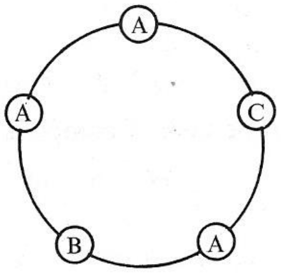
ROBLEM 1 Having enough beads to permit unlimited use of each of n colours, how many different necklaces consisting of p beads can be made, where p is prime?

We shall assume that the necklaces are produced by first forming a string of p beads and then joining the ends. Our first step is therefore to count how many different strings of p beads there are. Well that's fairly straightforward. There are n choices for the first bead, n choices for the second, and so on. In all there are n^p different strings.

Notice that, of these strings, n consist of beads of one colour alone (one such for each colour). Hence there are $n^p - n$ strings involving at least two colours. As the single colour necklaces are easily counted, we shall put these on one side and concentrate on the ones involving two or more colours.

As one must expect, strings counted differently in this way can result in the same necklace being produced. For example, the five strings of beads involving colours A, B and C illustrated below, all result in the same necklace.





Notice that the strings in this example are obtained from one another by removing the top bead and replacing it at the bottom of the string.

We shall call the operation of moving a bead from the top to the bottom of a string a 'move'. Two strings which can be obtained from each other by a sequence of moves clearly correspond to the same necklace. From a given string of p beads, how many different strings can be obtained by moves? The obvious answer is p, unless after some fewer number of moves the original colour scheme is restored. We use the Division Algorithm to show that this cannot happen.

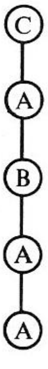
Let k be the least number of moves which restore the colour scheme of a string of p beads ($k > 1$ since we are ignoring strings of a single colour). By the Division Algorithm, there exist integers q and r such that

$$p = qk + r, \quad \text{where } 0 \leq r < k.$$

If k moves restore the colour scheme, then so too do $2k, 3k, \ldots, qk$ moves. Furthermore, p moves certainly restores the colour scheme, since each bead returns to its initial position. Therefore, after the qkth move only a further r moves are needed to restore the colour scheme, and since $r < k$, we are forced to conclude that $r = 0$. This in turn implies that k divides p, and since p is prime and $k > 1$ we must have $k = p$.

The outcome of this is that the $n^p - n$ strings involving two or more colours are partitioned into disjoint sets of p strings, each set consisting of all strings which can be obtained from each other by a sequence of moves. This means that $p | n^p - n$, which is Fermat's Little Theorem.

One might be tempted to conclude from this that there are in all $\dfrac{n^p - n}{p}$ different necklaces involving two or more colours and hence a total of $\dfrac{n^p - n}{p} + n$ different necklaces. Unfortunately there is a further complication which we have not taken into account. Consider the string shown. It is the first string of our earlier example but with order reversed (i.e. turned over). It gives rise to a further set of five strings which correspond to the same necklace (turned over) in the example.



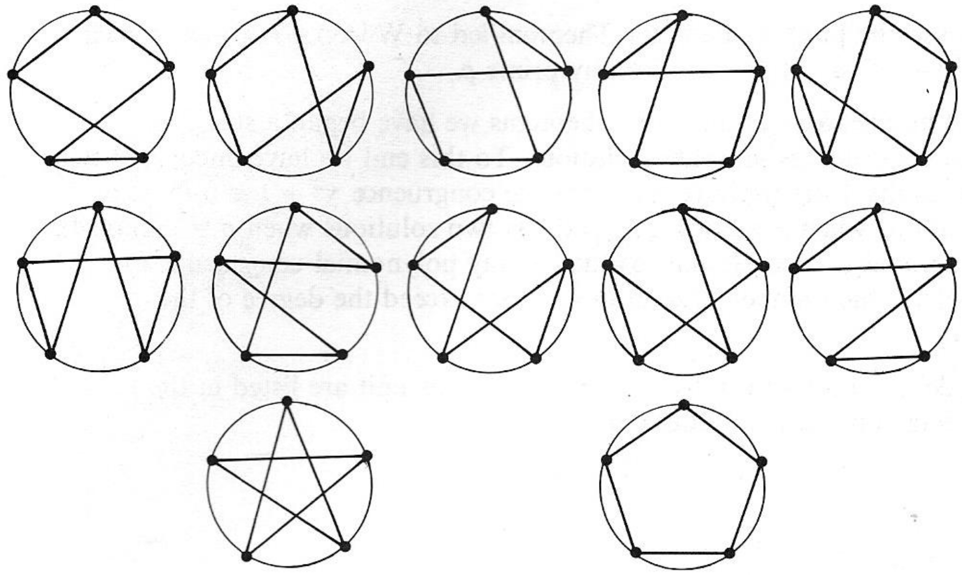
So, in general, two different sets of p strings might give rise to the same necklace. We say 'might' because turning a string over does not always produce a new string—or, put another way, some necklaces are symmetrical!

We leave you the task of completing Problem 1 as a challenge problem. For the record, the answer is $\dfrac{n^p - n}{2p} + \dfrac{n^{(p+1)/2} - n}{2} + n$. Notice that as this is an integer value, the first term still incorporates Fermat's Little Theorem.

A similar problem leads to an illustration of Wilson's Theorem.

ROBLEM 2 How many stellated p-gons are there?

A stellated n-gon is formed by placing n points at equal distances around the circumference of a circle and then joining these points with n straight-line segments, crossings being allowed. For $n = 5$, there are twelve stellated pentagons, as shown in the figure.



Notice that the five pentagons in the first row are congruent, being obtained from each other by rotations through $\frac{2\pi}{5}$. Similarly, the pentagons in the second row are congruent. The remaining two are the *regular* stellated pentagons, having rotation through $\frac{2\pi}{5}$ as a symmetry operation. Hence, if we classify stellated pentagons up to similarity (for we are not concerned about size) there are just *four* essentially different ones.

In the same way, we now want to count the number of different stellated p-gons, where p is a prime (greater than 2). We leave you to confirm the details, which are as follows.

Placing p points at equal distances around the circumference of a circle, the total number of stellated p-gons that can be formed by joining them (corresponding to the twelve for $p = 5$) is $\frac{1}{2}(p-1)!$. The number of regular ones is $\frac{1}{2}(p-1)$. [The regular stellated p-gons are formed by choosing an integer n in the range $1 \leq n \leq \frac{p-1}{2}$ and joining each point to the one n further round the circle, clockwise.] The remaining $\frac{1}{2}(p-1)! - \frac{1}{2}(p-1)$ irregular stellated p-gons are partitioned into congruent sets of p each, the members of each set being obtained from each other by rotations through $\frac{2\pi}{p}$. Hence there are in all

$$\frac{\frac{1}{2}(p-1)! - \frac{1}{2}(p-1)}{p} + \frac{1}{2}(p-1) = \frac{(p-1)! - (p-1)}{2p} + \frac{p-1}{2}$$

different stellated p-gons. As this is an integer, the first term illustrates that $p|(p-1)! - (p-1)$. That is, $(p-1)! \equiv (p-1) \equiv -1 \pmod{p}$, which is Wilson's Theorem.

4.6 Summary

After a brief look at Fermat's Factorization Method, the remainder of the unit hinged on Fermat's Little Theorem and its applications. The theorem says that for a prime p, if $p \nmid x$ then $x^{p-1} \equiv 1 \pmod{p}$. Catering for the case $p|x$ we have the Corollary that $x^p \equiv x \pmod{p}$ for all integers x.

A variation in the proof of Fermat's Theorem led to Wilson's Theorem, which says that $(p-1)! \equiv -1 \pmod{p}$ for any prime p.

Looking at applications of these two theorems we have begun a study of polynomial congruences and their solutions. To this end we have uncovered two important results. First we have seen that the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has no solutions when $p \equiv 3 \pmod{4}$ and has two solutions when $p \equiv 1 \pmod{4}$. Second, Lagrange's Theorem tells us that in any polynomial congruence to prime modulus, the number of solutions cannot exceed the degree of the polynomial.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

0 335 14010 6